UNITED STATES DISTRICT COURT
DISTRICT OF DELAWARE

IN RE GOOGLE INC. COOKIE PLACEMENT CONSUMER PRIVACY LITIGATION	C.A. No. 12-MD-2358 (SLR) **Jury Demand** CONSOLIDATED CLASS ACTION COMPLAINT
This Document Relates to: **All Actions**	

CLASS ACTION COMPLAINT

1. This class action lawsuit seeks damages and injunctive relief on behalf of similarly situated individuals domiciled in the United States who used the Apple Safari or Microsoft Internet Explorer web browsers and visited a website that deployed third-party tracking cookies from Google, Inc. ("Google") (through its DoubleClick advertising service), PointRoll, Inc. ("PointRoll"), Vibrant Media, Inc. ("Vibrant"), Media Innovation Group, LLC ("Media") or WPP, plc (Google, PointRoll, Vibrant, Media, and WPP are, collectively, "Defendants"). Those cookies circumvented Plaintiffs' and Class Members' browser settings that blocked such cookies. Defendants' secret and unconsented-to use of those cookies was part of the deception Defendants used to knowingly intercept and gain access to users' Internet communications and activity in violation of state and federal laws.

NATURE OF THE ACTION

2. Plaintiffs bring this consumer Class Action on behalf of themselves and a proposed class of similarly situated individuals (hereinafter "Class Members"), victimized by Defendants' unfair, deceptive, and unlawful business practices. The Defendants violated the Plaintiffs' and Class Members' privacy and security rights, and financial interests, by illegally intercepting, gaining unauthorized access to, and using and retaining Plaintiffs' and Class Members' data contained on and/or produced by their computing devices. These devices include

computers and mobile electronic devices used for communication, Internet, and multimedia capabilities (hereinafter referred to collectively as "Computing Devices").

3. Acting intentionally and secretly, Defendants circumvented the set "do not track" privacy settings on Plaintiffs' and Class Members' Computing Devices in order to obtain Personally Identifiable Information ("PII") without notice or permission, and for commercial gain.

4. Defendants' surreptitious circumvention of Plaintiffs' and Class Members' privacy controls in order to obtain PII without notice or permission and tracking violates the following statutes and gives rise to Plaintiffs' and Class Members' causes of action:

I) the Electronic Communication Privacy Act, 18 U.S.C. § 2510, *et seq.* (the "Wiretap Act");

II) the Stored Communications Act, 18 U.S.C. § 2701, *et seq.* (the "SCA");

III) the Computer Fraud and Abuse Act, 18 U.S.C § 1030 (the "CFAA");

IV) Invasion of Privacy;

V) Intrusion upon Seclusion;

VI) California Unfair Competition Law, Business and Professions Code § 17200, *et seq.* (the "UCL");

VII) California Computer Crime Law, Penal Code § 502 (the "CCCL");

VIII) California Invasion of Privacy Act, Penal Code § 630, *et seq.* (the "CIPA"); and

IX) California Consumers Legal Remedies Act, Civil Code § 1750, *et seq.* (the "CLRA").

JURISDICTION AND VENUE

5. This Court has general personal jurisdiction over Defendants because: Google, Inc., PointRoll, Inc., and Vibrant Media, Inc. are incorporated under the laws of Delaware; Media Innovation Group, LLC is a Delaware limited liability company; and WPP controls a Delaware LLC (Media Innovation Group) and regularly conducts business throughout the United

States, including Delaware. The Court also has specific personal jurisdiction over all Defendants because their actions caused injury to Delaware-domiciled members of the purported class.

6. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because this action arises in part under federal statutes, namely the Wiretap Act, the CFAA, the SCA, and, pursuant to 28 U.S.C. § 1332(d) under the Class Action Fairness Act, because the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and a member of the class is a citizen of a State different from any defendant.

7. This Court has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367 because the state law claims form part of the same case or controversy under Article III of the United States Constitution.

8. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because have minimum contacts in Delaware sufficient to subject them to the personal jurisdiction of this Court.

9. Venue is also proper in this District pursuant to 28 U.S.C. § 1407 because this case was transferred to this District for consolidated pretrial proceedings by the United States Judicial Panel on Multidistrict Litigation.

THE PARTIES

10. Plaintiff William Gourley is an adult domiciled in McCracken county, Kentucky, who used the Apple Safari and Internet Explorer web browsers with the default privacy settings to interact with the Internet[1] for uses including reviewing and transmitting confidential and personal information and visited websites with third-party advertisements of the Defendants.

[1] Including, but not limited to, the following definition of the Internet from *In re DoubleClick Inc. Privacy Litig*., 154 F. Supp. 2d 497, 500-02 (S.D.N.Y. 2001):

> *The Internet is accurately described as a "network of networks." Computer networks are interconnected individual computers that share information. Anytime two or more computer networks connect, they form an "internet." The "Internet" is a shorthand name for the vast collection of interconnected computer networks that*

11. Plaintiff Jose M. ("Josh") Bermudez is an adult domiciled in New Haven county, Connecticut, who used the Apple Safari web browser with the default privacy settings to interact with the Internet for uses including reviewing and transmitting confidential and personal information and visited websites with third-party advertisements of Defendants Google, Vibrant, and PointRoll.

12. Plaintiff Nicholas Todd Heinrich is an adult domiciled in Napa county, California, who used the Apple Safari web browser with the default privacy settings to interact with the Internet for uses including reviewing and transmitting confidential and personal information and visited websites with third-party advertisements of the Defendants.

13. Plaintiff Lynne Krause is an adult domiciled in Philadelphia county, Pennsylvania, used the Apple Safari web browser with the default privacy settings to interact with the Internet for uses including reviewing and transmitting confidential and personal information and visited websites with third-party advertisements of Defendants Google, Media, and PointRoll.

---

evolved from the Advanced Research Projects Agency Network ("ARPANet") developed by the United States Defense Department in the 1960's and 1970's. Today, the Internet spans the globe and connects hundreds of thousands of independent networks.

The World Wide Web ("the Web" or "WWW") is often mistakenly referred to as the Internet. However, the two are quite different. The Internet is the physical infrastructure of the online world: the servers, computers, fiber-optic cables and routers through which data is shared online. The Web is data: a vast collection of documents containing text, visual images, audio clips and other information media that is accessed through the Internet. Computers known as "servers" store these documents and make them available over the Internet through "TCP/IP" (Transmission Control Protocol/Internet Protocol), a set of standard operating and transmission protocols that structure the Web's operation. Every document has a unique "URL" (Universal Resource Locator) that identifies its physical location in the Internet's infrastructure. Users access documents by sending request messages to the servers that store the documents. When a server receives a user's request (for example, for Lycos.com's home page), it prepares the document and then transmits the information back to the user.

14. Defendant Google is a publicly traded Delaware corporation with headquarters at 1600 Amphitheatre Parkway, Mountain View, CA 94043 and does business throughout the United States. Providing an array of Internet products, Google has an enormous Internet presence. Underscoring its vast Internet reach, Google describes its "mission" as "to organize the world's information and make it universally accessible and useful."[2] In June 2011, comScore, an Internet analytics company, put Google's worldwide reach at 1 billion unique visitors per month.[3] Google obtains the majority of its profits from advertising. Confirming advertising's central importance to Google's business, Google's "Ten Things We Know to be True" – sometimes called Google's "Ten Commandments" – states that "[h]undreds of thousands of advertisers worldwide use [Google] Adwords to promote their products; hundreds of thousands of publishers take advantage of our AdSense program to deliver ads relevant to their site content."[4]

15. Defendant PointRoll, a subsidiary of the Gannett media company, is a Delaware corporation with headquarters at 951 East Hector Street, Conshohocken, PA 19428. Doing business throughout the United States, PointRoll's website homepage describes PointRoll as "the leading provider of digital marketing solutions and technology" that "[p]ower[s] the most effective digital campaigns by delivering both the art and science of consumer engagement."[5] Touting its ability to provide "targeting" of advertisements to computer users, PointRoll emphasizes the "memorable and measurable impression" its advertising campaigns provide for clients.[6]

---

[2] *Google Company Overview*, http://www.google.com/about/company/ (last visited Dec. 14, 2012) (All websites last visited on Dec. 14, 2012, unless otherwise stated).

[3] COMSCORE DATA MINE, *Google Reaches 1 Billion Global Visitors* (June 22, 2011), http://www.comscoredatamine.com/2011/06/google-reaches-1-billion-global-visitors/.

[4] *Google: What We Believe, "Ten Things We Know to Be True,"* http://www.google.com/about/company/philosophy/.

[5] POINTROLL, http://www.pointroll.com.

[6] *Id.*

16. Defendant Vibrant Media, Inc. is a Delaware corporation, headquartered in New York, New York. Founded in 2000, with offices in New York, San Francisco, Detroit, Chicago, Los Angeles, Boston, Atlanta, London, Paris, Hamburg, Munich and Dusseldorf, Vibrant's website "Overview" describes the company as "the world's leading provider of in-content contextual advertising that gets brand content and advertising discovered across platforms."[7]

17. Defendant Media Innovation Group, LLC, a Delaware limited liability company headquartered in New York, New York, describes itself as combining technology and marketing expertise "to equip unique brands with unique capabilities in the digital sphere. Media Innovation Group is a born-digital market leader that understands marketing."[8]

18. Defendant WPP plc, a public limited company with its main offices in Dublin, Ireland, and London, United Kingdom, owns Defendant Media Innovation Group, LLC.[9]

FACTUAL ALLEGATIONS

THE DEFENDANTS

19. **Google.** According to Google's 10-K filing for the fiscal year ending December 31, 2011, Google "is a global technology leader focused on improving ways people connect with information."[10] That same filing revealed that Google "generate[s] revenue primarily by delivering relevant, cost-effective online advertising."[11] The February 17, 2012 *Wall Street Journal* article that revealed Google's actions that forms the basis of this lawsuit stated that

---

[7] VIBRANT OVERVIEW, http://www.vibrantmedia.com/about/index/asp.

[8] MEDIA INNOVATION GROUP, INNOVATION, http://www.themig.com/en-us/organization.html.

[9] *See, e.g.,* WPP, *What We Do*, http://www.wpp.com/wpp/about/whatwedo (listing digital offerings delivered through WPP Digital); WPP, Our Companies, http://www.wpp.com/wpp/companies/ (providing list of WPP companies); Media Innovation Group, Account Coordinator – New York job listing, http://www.themig.com/docs/opportunities/Account_Coordinator_NY.pdf (states, in pertinent part: *Behind Media Innovation Group is the world's largest buyer of media, WPP*.).

[10] http://investor.google.com/pdf/20111231_google_10K.pdf.

[11] *Id*.

according to comScore Media Metrix[12] Google delivered web ads viewed at least once by 93% of United States web users in December 2011.[13]

20. **PointRoll.** PointRoll is a leading provider of online advertising that claims to "[p]ower[] 55% of all rich media campaigns online" and "serve over 450 billion impressions for more than two-thirds of the Fortune 500 brands."[14] According to a February 17, 2012 Washington Post article, "PointRoll…speciali[zes] in digital circulars and other 'rich media' ads such as videos. PointRoll says that it is the leading rich media advertiser on the Web and works on mobile and Web ads."[15]

21. Web analytics firm Quantcast estimates that PointRoll powers more than 50 percent of all rich media campaigns on line.[16] "Rich media" is, at bottom, enhanced Internet advertising. One example is "streaming video," where a user clicks on a promotion for a movie and gets a streaming video segment from that movie. Another example is the use of "applets," programs embedded in advertising that create interaction between the user and the advertisement, such as when the user moves his cursor over a particular website area and the cursor becomes an image, such as a symbol for a product, or, as on the site www.whatis.com, becomes a red question mark.[17]

---

[12] Described as the *Industry-Leading Online Audience Measurement and Media Planning Solution*, COMSCORE, http://www.comscore.com/Products/Audience_Analytics/Media_Metrix.

[13] Julia Angwin & Jennifer Valentino-Devries, *Google's iPhone Tracking: Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy*, WALL ST. J., (Feb. 17, 2012) *available, at*, http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html (hereinafter "Angwin & Valentino-Devries WSJ Article").

[14] POINTROLL, *About Us*, http://www.pointroll.com.

[15] Hayley Tsukayama, *Who are Vibrant Media, WPP and PointRoll*, WASH. POST (Feb. 17, 2012) http://articles.washingtonpost.com/2012-02-17/news/35442628_1_pointroll-privacy-settings-web-ads (hereinafter "Tsukayama Article").

[16] *Id.*

[17] *See, e.g.*, WHATIS.COM, *Definition: Rich Media*, http://whatis.techtarget.com/definition/rich-media. *See also* Tig Tillinghast, *Rich Media Campaigns: The Pros and Cons*, CLICKZ: MARKETING NEWS & EXPERT ADVICE (Apr. 27, 2001), http://www.clickz.com/clickz/column/1703376/rich-media-campaigns-the-pros-cons.

22. PointRoll, by its own admission, has "joined with Google to enable PointRoll's advertisers to run rich media ad campaigns across the Google content network."[18] Benefits of the Google-PointRoll partnership are summarized in PointRoll's press release: "PointRoll clients can now take advantage of the company's full-service offering, including creative services, ***targeting, and extensive tracking*** and measurement capabilities on a significantly expanded number of websites."[19]

23. Google and PointRoll confirm their agreement and provide their assurances about advertising standards when they work together: "Google and PointRoll worked together to ensure that the ads served to the Google content network meet Google's policies and specifications."[20]

24. **Vibrant Media.** According to the Tsukayama Article, "Vibrant Media is known for its in-text ads, aka those double-underlined mouseover ads that pop up in the text of articles on the web." Vibrant's reach is vast. The company's website boasts of having "over 6,600 premium publishers, reaching more than 300 million unique users per month (comScore, 2012)."[21] A big part of Vibrant's business is advertising specifically targeted to potential customers identified by previously compiled data dossiers about those customers, their characteristics, likes and dislikes. Vibrant's website "Overview" confirms this central focus: "Vibrant gives top brand marketers the opportunity to deliver highly targeted advertisements and branded content within text and images. Vibrant works with top brand advertisers such as Hewlett-Packard, Microsoft, P&G, Sainsbury's and Unilever."[22] Vibrant claims its "[i]ndustry leading contextual products and technology allow premium advertisers to align their brand

[18] POINTROLL PRESS RELEASE, *Industry Leader PointRoll to Serve Ads on the Google Content Network*, (May 19, 2008), http://showcase.PointRoll.com/press_release_080519.aspx.

[19] *Id.* (emphasis added).

[20] *Id.*

[21] VIBRANT OVERVIEW, http://www.vibrantmedia.com/about/index.asp.

[22] *Id.*

advertising with relevant content images, news & video to reach and engage target audiences."[23] Vibrant touts its ability to place brands of its "over, 6,600 global partners" "in the most relevant editorial content to reach their target audiences."[24] In other words, Vibrant places its advertising clients' messages where the right, specifically targeted audiences, will see them. To do that, Vibrant needs first to identify those specific audiences.

25. **Media Innovation Group.** More clearly describing its offerings, Media says that "[a]s data driven marketing becomes the norm," Media "provide[s] total visibility into every corner of the digital market space," so that "advertisers know exactly what they're buying."[25] Like Vibrant, Media promises clients that their advertisements will be seen by precisely the right audiences: "For [our] clients, this is like owning an integrated circuit for their entire marketplace. Our technology stack enables us to value, buy, and optimize any – or every – digital connection with singular precision, affording clients universal reach with pinpoint control. The soul of the enterprise is an enormously powerful data management system that understands how your brand users are responding to a myriad of digital experiences."[26] In plain English, Media tells clients that Media knows exactly to whom the clients ought to be pitching their advertisements. Defendant Media says, in posting employment openings: "Behind Media Innovation Group is the world's largest buyer of media, WPP."[27] Media's then-GM Brian Lesser, in a June 2010 interview, stated that "MIG is WPP's technology-driven digital marketing company…our goal is to build technology and leverage data to give agencies and advertisers access to the audiences they are trying to reach."[28]

---

[23] *Id.*

[24] *Id.*

[25] MEDIA INNOVATION GROUP, *Strategy: Certainty*, http://www.themig.com/en-us/strategy.html#certainty.

[26] MEDIA INNOVATION GROUP, TECHNOLOGY, http://www.themig.com/en-us/technology.html.

[27] MEDIA INNOVATION GROUP, *Account Coordinator – New York job listing*, http://www.themig.com/docs/opportunities/Account_Coordinator_NY.pdf .

[28] Brian Lesser, *WPP's Media Innovation Group GM Brian Lesser On DSPs, Holding Cos And*

26. **WPP.** WPP, which owns Defendant Media, describes itself as "the world leader in marketing communications services."[29] WPP has 3,000 offices, 162,000 employees, operates in 110 countries, and owns a number of media, marketing, advertising, public relations and similar firms.[30]

HOW TARGETED INTERNET ADVERTISING WORKS

27. Not essential for stating Plaintiffs' claims, the following description of how the Internet and targeted advertising works provides information about the methods Defendants used to violate the Plaintiffs' privacy and security rights.

28. Internet users' web browsers (sometimes just "browsers") permit users to interact with – or "surf" – the Internet. Internet users use web-browser software to access, communicate on, and navigate the Internet. Popular web browsers include Apple Safari, Microsoft Internet Explorer ("IE"), Google Chrome, and Mozilla Firefox.

29. Web browser companies compete for users based, among other things, on the ability of the company's browser to provide a secure environment for the user's Internet activities.

30. Every website is hosted by a server. Servers communicate with the web browsers of individual Internet users to display the contents of webpages on the monitors of users' computing devices.

31. When an Internet user requests the contents of a webpage by typing the address of the webpage into the navigation bar of their chosen web browser and pressing "enter," or by

---

Launching ZAP 3.0, ADEXCHANGER (June 10, 2012), http://www.adexchanger.com/agencies/wpp-group-mig/.

[29] WPP, *WPP at a Glance*, http://www.wpp.com/wpp/about/wppataglance.

[30] *Id.*

clicking on a link, the browser responds by sending a "GET" command to the server that hosts the requested webpage. The "GET" command is designed to retrieve information from the server, and instructs the server to send the information contained on the relevant webpage to the user's browser for display on the monitor of the user's computing device.

32. Although a single webpage appears on a user's screen as a complete product, each of the different parts of a webpage – e.g., the text, pictures, advertisements, sign-in box – often exist on separate servers.

33. Messages between clients and servers are sent in IP packets, whereby servers send the different parts of a requested webpage to the requesting user's computing device. This involves the dividing up of the requested information into discrete "packets," which generally consist of a "header," the "body" or "payload."[31] The header is sometimes described as "control data." It provides information about the message itself, but does not constitute the contents of the message. For example, headers often provide instructions about the packet's contents, source and destination, such as the requester's IP address, the sender's IP address, the number of packets comprising the response, the packet's identification number, the particular protocol in use for the communication – the Internet uses the Internet Protocol Suite - and other information. Sometimes referred to as "user data," the packet's body or payload is the actual substantive information content the user requested, for example, text or a picture.

34. Using network switches and routers, packets are routed to the user's computing device where the disparate packets are finally assembled in the proper order.[32]

---

[31] *See, e.g.*, THE LINUX INFORMATION PROJECT, *Packet Switching Definition*, http://www.linfo.org/packet_switching.html.

[32] *See, e.g.*, Bradley Mitchell, *What Is Packet Switching on Computer Networks?*, ABOUT.COM GUIDE, http://compnetworking.about.com/od/networkprotocols/f/packet-switch.htm.

35. During routing, packets can be routed out of order, and across a variety of routes, before reaching their final destination. For one requested webpage for a user in Wilmington, Delaware, packets might come from a server in New York via Seattle, others from a server in Los Angeles via Chicago, and so on. Packets move extremely quickly through the network.

36. Routers and computers exist on both ends of an electronic message – they arrange and re-arrange packets as necessary, and as needed re-send packets to ensure that at least one copy of a message's multiple packets reaches its final destination.

37. When the Internet was in its infancy, advertising on websites followed the same model as traditional newspapers. Advertisers paid for ads, often called "banner ads," to be placed on specific pages based on the content of the page rather than personalized information about the individual user accessing the page.

38. Internet "cookies" were soon developed, which could be used to track an individual person's activities and communications on a particular website, as well as across the Internet.

39. In general, cookies are categorized by (1) the length of time for which they are placed on a user's device, and (2) the party who places the cookie on the user's device:

a. Cookie Classifications by Time

i. "Session cookies" are placed on the user's computer for the time period in which the user is "reading and navigating the website" that placed the cookie. Web browsers normally delete session cookies when the user closes the browser.

ii. "Persistent cookies" are designed to survive past one browser session of a user. The lifespan of a persistent cookie is set by the person

who creates the cookie. As a result, a "persistent cookie" could stay on a user's device for years. Persistent cookies can be used to track users' actions on the Internet, and are also sometimes referred to as "tracking cookies."

b. Cookie Classifications by Party

i. "First-party cookies" are those set on a user's device by the website the user is visiting at the time the cookie is set on the device. For example, when a user visits YellowPages.com, the website will set a collection of Yellow Pages (first party) cookies on her device. First-party cookies can be helpful to both the user and a given server and/or website to assist with security, log-in, and other functionality.

ii. "Third-party cookies" are set on a user's device by a website other than the site the user is visiting at the time the cookie is set. For example, the same user who visits YellowPages.com will also have cookies placed on her device by third-party websites, including advertising companies which track user behavior, like Google, PointRoll, Vibrant, and Media. Unlike first-party cookies, third-party cookies are not typically helpful to either the user or the given server and/or website. Instead, third-party cookies typically work in furtherance of targeted advertising.

40. As computer programming became more advanced and the use of "cookies" was further developed, new businesses were created to use sophisticated database systems based on numerous cookies that could track activities and communications for the purposes of selling advertising targeted specifically to an individual person. With these advances, website owners,

the digital-age equivalent of newspaper publishers, could sell advertising space to these new businesses to place other companies' ads, customized based on each individual user's Internet browsing history.

41. Most commercial websites with extensive advertising allow third-party companies such as Google, PointRoll, Vibrant, and Media to serve advertisements on the commercial entities' websites directly from the third-party company's servers rather than going through the individual website's server. The host website leaves part of its webpage blank where the third-party advertisements will appear. Upon receiving a "GET" request from a user seeking to display a particular webpage, the server for that webpage will subsequently respond to the browser, instructing the browser to send a "GET" request to the third-party company charged with serving the advertisements for that particular webpage. Some websites contract with multiple third-parties to serve ads such that the website will simultaneously instruct the user's browser to send multiple GET requests to multiple third-party websites. Advertisements provided by these third-parties are then injected into the host webpages in the places left open by the hosts. In many cases, the third party receives the GET request and a copy of the user's request to the first-party website before the content of the user's initial request from the first-party webpage shows up on the user's screen. The third-party server responds to the GET request by sending the advertisement to the user's browser, which then displays it on the user's device. The entire process occurs within milliseconds and the third-party content appears to arrive simultaneously with the first-party content so that the user does not discern any separate GET requests from the third-parties.

42. In addition to the "GET" command, another important basic command used by web browsers is the "POST" command. The POST command is designed to request a web

server to accept data for storage which is enclosed in a message sent from a user's browser to the server. The POST command is used when users complete forms on the web to send information to the webpage with which they are attempting to communicate. For example, a browser would use the POST command to send information a user filled out in a form containing her personally identifiable information for purposes of creating an account on a webpage.

43. Online advertising companies like Defendants do more than simply inject ads onto webpages. They also offer marketers the ability to find consumers and deliver targeted, relevant and engaging advertisements that improve ad effectiveness. PointRoll, for example, claims: "PointRoll has evolved beyond the banner [advertisement] to offer marketers the ability to find the right consumers at the right time and deliver a relevant and action-inspiring advertising experience across multiple digital touch points."[33]

44. The Defendants seek specifically to target advertisements to particular potential Internet-user customers based on data collected about those users while at the same time continuing to collect ever-increasing amounts of data about those users further to expand the Defendants' databases of user information, and, in turn, further to refine marketing pitches and advertisements focused to particular users, which, finally, enables the Defendants to charge more for their services and make more money.

45. To inject the most targeted ads possible, and therefore charge higher rates to buyers of the ad space, these third-party companies must also use computer code to compile the Internet histories of users. The third-party advertising companies use "third-party cookies" to accomplish this goal. In the process of injecting the advertisements into the first-party websites, the third-party advertising companies also place third-party cookies on user's computing devices.

[33] *About PointRoll*, http://blog.pointroll.com/about-pointroll/.

Since the advertising companies place advertisements on multiple sites, these cookies allow these companies to keep track of and monitor an individual user's web activity over every website on which these companies inject ads.

46. These third-party cookies are used by advertising companies to help create detailed profiles on individuals, including, but not limited to an individual's unique ID number, IP address, browser, screen resolution, and a history of all websites visited within the ad network by recording every communication request by that browser to sites that are participating in the ad network, including all search terms the user has entered. The information is sent to the companies and associated with unique cookies -- that is how the tracking takes place. The cookie lets the tracker associate the web activity with a unique person using a unique browser on a device. Once the third-party cookie is placed in the browser, the next time the user goes to a webpage with the same Defendant's advertisements, a copy of that request can be associated with the unique third-party cookie previously placed. Thus the tracker can track the behavior of the user, and in the case of Plaintiffs and Class Members, do so despite Plaintiffs and Class Members privacy settings in place to block this tracking scheme, as described below. Defendants' actions that form the basis of this lawsuit allowed Defendants to illegally place these third-party cookies for future tracking purposes.

47. Websites can be identified by the Internet's address system, which depends centrally on Uniform Resource Locators ("URLs"). A URL, for example, can consist of the familiar http://www.ca3.uscourts.gov/. Many URLs, however, convey much more information than a mere web address that offers a variety of different potential informational avenues to a visitor. For example, the URL http://incest-survivors.supportgroups.com/ is highly informative. The very name of the site unmistakably signifies the site's content. Many users visiting that site,

and others like it, are signifying a highly personal private interest.

48. By observing the web activities and communications of literally tens of millions of Internet users, the advertising companies build digital dossiers of each individual user's "digital self,"[34] the user's interests, concerns, hobbies, politics, preferences, and shopping activities, tagging each individual user with a unique identification number used to aggregate the user's web activity.

Value of Personal Information

49. The monetary and trade value of the information that Defendants take from users is well understood in the e-commerce industry. Personally identifiable information ("PII") is now viewed as a form of currency. Professor Paul M. Schwartz noted in the Harvard Law Review:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.[35]

50. Another recent article put the point even more succinctly: "PII is now a commodity that companies trade and sell."[36]

---

[34] *See, e.g.,* Gordon Bell & Jim Gemmell, *Our Digital Selves*, N.Y. TIMES (Nov. 25, 2012), http://www.nytimes.com/roomfordebate/2012/11/25/will-diaries-be-published-in-2050/lifelogging-requires-a-human-touch.

[35] Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2056-57 (2004).

[36] John T. Soma, et al., *Corporate Privacy Trend: The 'Value' of Personally Identifiable Information ("PII") Equals the 'Value' of Financial Assets,* XV RICH. J.L. & TECH. 1 (2009) ("Soma Article"), at 1 (citing C. Ciocchetti, *The Privacy Matrix*, 12 J. TECH. L. & POL'Y 245, 247 (2007); M. Kightlinger, *The Gathering Twilight? Information Privacy on the Internet in the Post-Enlightenment Era*, 24 J. MARSHALL J. COMPUTER & INFO. L., 353, 384 (2006)).

51. The Soma Article further states: "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[37]

52. Likewise, in the *Wall Street Journal*, privacy expert and then-fellow at the Open Society Institute, Christopher Soghoian, confirms the incentive for the Defendants' illegal hack of Safari's do-not-track protection:

> The dirty secret of the Web is that the "free" content and services that consumers enjoy come with a hidden price: their own private data. Many of the major online advertising companies are not interested in the data that we knowingly and willingly share. Instead, these parasitic firms covertly track our web-browsing activities, search behavior and geolocation information. Once collected, this mountain of data is analyzed to build digital dossiers on millions of consumers, in some cases identifying us by name, gender, age as well as the medical conditions and political issues we have researched online.
>
> Although we now regularly trade our most private information for access to social-networking sites and free content, the terms of this exchange were never clearly communicated to consumers.[38]

53. Behaviorally targeted advertisements based on a user's tracked Internet activity generally sell for at least *twice* as much as non-targeted, run-of-network ads.[39]

54. In the behavioral advertising market, "the more information is known about a consumer, the more a company will pay to deliver a precisely-targeted advertisement to him."[40]

55. Upon information and belief, most of the Defendants' advertising clients pay on a

---

[37] *Id.* at 2.

[38] Julia Angwin, *How Much Should People Worry About the Loss of Online Privacy?*, WALL ST. J. (Nov. 15, 2011), *available at*, http://online.wsj.com/article/SB10001424052970204190704577024262567105738.html.

[39] *Network Advertising Initiative, Study Finds Behaviorally-Targeted Ads More Than Twice As Valuable, Twice As Effective As Non-Targeted Online Ads*, (Mar. 24, 2010), http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf.

[40] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers*, FEDERAL TRADE COMM'N, at 37, (Dec. 2010), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

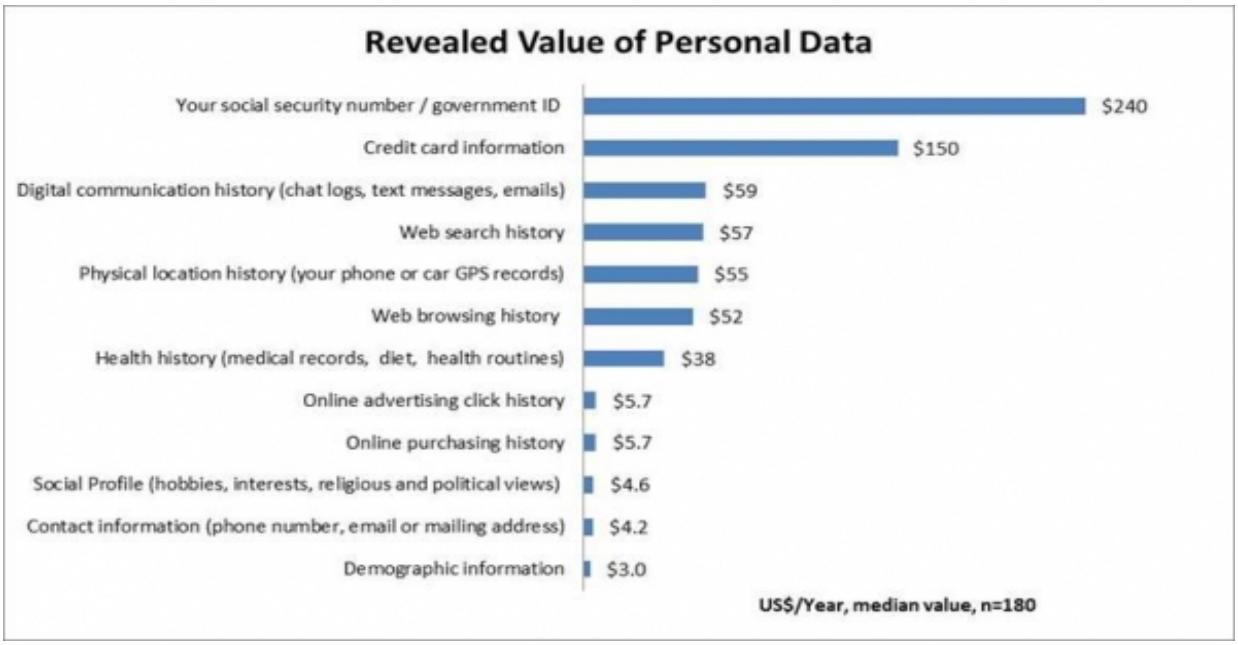
cost-per-click basis. The Defendants also offer cost-for-impression ads, which charge an advertising client each time a client's ad displays to a user. In general, behaviorally-targeted advertisements can produce up to 670 percent more clicks on ads per impression than run-of-network ads.[41] Behaviorally-targeted ads are also over twice as likely to convert users into buyers of an advertised product as compared to run-of-network ads.[42]

56. The cash value of users' personal information can be quantified. For example, in a recent study authored by Tim Morey, researchers studied the value that 180 Internet users placed on keeping personal data secure. Contact information was valued by the study participants at approximately $4.20 per year. Demographic information was valued at approximately $3.00 per year. Web browsing histories were valued at a much higher rate: $52.00 per year. The chart below summarizes the findings:[43]

[41] Howard Beales, *The Value of Behavioral Advertising*, at 11, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf (2010).

[42] *Id.* at 3.

[43] Tim Morey, *What's Your Personal Data Worth?*, DESIGN MIND, (Jan. 18, 2011), http://designmind.frogdesign.com/blog/what039s-your-personal-data-worth.html .



57. Defendant Google now offers users the opportunity to join a panel called "Google Screenwise Trends," which, according to Google, is designed "to learn more about how everyday people use the Internet."[44]

58. Upon becoming a panelist, Internet users add a browser extension that will share with Google the sites that users visit and how the panelist uses them. The panelist consents to Google tracking this information for three months in exchange for one of a number of "gifts," including gift cards to retailers such as Amazon.

59. After three months, Google also agrees to pay panelists additional unspecified gifts "for staying with" the panel.

60. These gift cards, mostly valued at exactly $5, demonstrate conclusively that Internet industry participants, including Defendants, understand and can quantify the financial value in Internet users' browsing habits.

---

[44] *See, e.g.*, Matt McGee, *Google Screenwise: New Program Pays You To Give Up Privacy & Surf The Web With Chrome*, SEARCH ENGINE LAND (Feb. 8, 2012), http://searchengineland.com/google-screenwise-panel-open-110716.

61. Facebook's initial public stock offering also demonstrated the market value of PII. A February 15, 2012 article in *The Financial Times* stated: "Two weeks ago Facebook announced an initial public offering that could value the company at up to $100 [billion]. Facebook is worth so much because of the data it holds on its 845 [million] users."[45]

62. Another confirmation of the monetizable nature of PII appeared in the February 17, 2012 Angwin and Valentino-Devries *Wall Street Journal* article: "[t]rade in personal data has emerged as a driver of the digital economy. Many tech companies offer products for free and get income from online ads that are customized using data about consumers. These companies compete for ads, in part, based on the quality of the information they possess about users."[46]

63. Moreover, active markets exist all over the world for this type of data. For instance, a company in the United Kingdom, Allow Ltd., has created a business model based on the value of personally identifiable information. When a customer signs up for Allow Ltd. the company sends a letter on behalf of its new client to the top companies in the United Kingdom that harvest personal data demanding that those companies immediately stop using the client's personally identifiable data.

64. A February 28, 2011 *Wall Street Journal* article stated that Allow, Ltd. paid one user $8.95 for permitting Allow to tell a credit card company that the user was looking for a new credit card.[47] Allow is one of a number of companies that offer users a real market for their personal information. That same *Wall Street Journal* article described the new company

---

[45] Richard Falkenrath, *Google Must Remember Our Right to be Forgotten*, FIN. TIMES (Feb. 15, 2012), http://www.ft.com/cms/s/0/476b9a08-572a-11e1-869b-00144feabdc0.html#axzz2F4G7Qqnv.

[46] Angwin & Valentino-Devries WSJ Article, http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html.

[47] Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, WALL ST. J. (Feb. 28, 2011), *available at,* http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html.

IntelliProtect. Demonstrating further the clear attribution of specific dollar values to PII, for a fee of $8.95 per month IntelliProtect prevents users from seeing ads based on private information.[48]

65. Another start-up, Enliken, "enables people to sell themselves to advertisers directly," and values a user's data at $12 per year. This again illustrates a market in which users can actually sell their Personally Identifiable Information, indicating that its value can be realized.[49]

66. The company Privacy Choice has a program called PrivacyFix, which measures the value that users are paying for the exchange "where companies are able to take user data, sell it to advertisers, and make money that allows them to give themselves a paycheck while keeping [users] afloat in free digital services." PrivacyFix measures users' last 60 days of activity on Google, extrapolates it to a year, and uses a value-per-search estimate. Privacy Choice's founder, Jim Brock, boasts that his Google value "checks in at more than $700 per year."[50]

67. Advertisers highly covet personal user data because such private information is not readily available. Defendants discovered a way to get this personal information, even from the Plaintiffs and Class Members who sought to block the disclosure of such information.

Allegations as to Safari Browser Users

68. Apple Safari is the web browser provided with Apple Computing Devices including the iPhone, iPad, iPod Touch, or Apple Mac computer as the default web browser.

---

[48] *Id.*

[49] Melissa Knowles, *Startup Gives Users Control Over Sale of Personal Data*, YAHOO! BLOG (October 3, 2012), http://news.yahoo.com/blogs/trending-now/startup-gives-users-control-over-sale-personal-data-194752267.html.

[50] Joe Mullin, *How Much Do Google and Facebook Profit From Your Data?*, ARS TECHNICA, (Oct. 9, 2012), http://arstechnica.com/tech-policy/2012/10/how-much-do-google-and-facebook-profit-from-your-data/.

69. Apple specifically advertised and continues to advertise to users that its Safari web browser has default settings that protected user privacy without users having to do anything. From the Apple Safari "Features" web page:

> Cookie Blocking – Some companies track the cookies generated by the websites you visit, so they can gather and sell information about your web activity. ***Safari is the first browser that blocks these cookies by default***, better protecting your privacy. Safari accepts cookies only from websites you visit.[51]

70. On another page, Apple informs users that its Safari browser allows for a "worry-free web," stating, "[t]o prevent companies from tracking the cookies generated by the websites you visit, ***Safari blocks third-party cookies by default***."[52]

71. Safari's "Privacy" preference settings inform Safari users that the browser will "Block cookies: From third parties and advertisers."

72. Every iPhone, iPad, iPod Touch, and Mac computer ships to the user with these default settings in Safari turned on to block cookies from third parties and advertisers.

73. By using Safari in default mode, which is set to block third-party cookies, users deny third parties and advertisers access to their Computing Devices for the purpose of placing cookies and tracking their behavior.

74. On February 17, 2012, the *Wall Street Journal* reported "Google Inc. and other advertising companies have been bypassing the privacy settings of millions of people using Apple's Inc.'s Web browser on their iPhones and computers - tracking the Web-browsing habits of people who intended for that kind of monitoring to be blocked."[53]

75. The *Wall Street Journal* article was based on the work of a Stanford computer science and law graduate student named Jonathan Mayer who revealed a scheme by which

---

[51] *Safari Features, Security and Privacy*, http://www.apple.com/safari/features.html#security (emphasis added).

[52] *What is Safari, Security*, http://www.apple.com/safari/what-is.html#security (emphasis added).

[53] Angwin & Valentino-Devries WSJ Article, http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html.

Defendants were bypassing the privacy settings of tens of millions of people who use Apple's Safari web browser to use the Internet.[54]

76. Safari's default settings provide an exception to the third-party cookie blocking privacy protection for situations where a user interacts in some way with a third party, including through the submission of a form to the third-party's website servers.

77. Google and the other Defendants exploited this exception by adding coding to ads that tricked Safari into believing the exception had been satisfied and that the user had submitted a form to Google or the other Defendants – even though there was, in fact, no such form submitted by the actual user.

78. The following illustrations from the February 17, 2012 Angwin and Valtentino-Devries *Wall Street Journal* article illustrate how this worked, using Google as an example:

[54] Jonathan Mayer, *Safari Trackers*, WEB POLICY BLOG, (Feb. 17, 2012), http://webpolicy.org/2012/02/17/safari-trackers/ (hereinafter "Mayer Study").

Tracking Leaves a Trail

For several months, Google used special code to place a tracking tool called a cookie on the computers and gadgets of people who used Apple's Safari Web browser, despite the fact that Safari usually blocks such tracking. Here's how it worked.

```
<script>var onDrtLoad = function() {if (typeof posWidgetIframeList != \'undefined\' && posWidgetIframeList) {for (var i = 0; i <
posWidgetIframeList.length; i++) {posWidgetIframeList[i].G_handleAdDoritosFlowDone();}}};</script><iframe frameborder=0 height=0 width=0
src=\"http://googleads.g.doubleclick.net/pagead/drt/s\" style=\"position:absolute\" onload=\"onDrtLoad()\"></iframe></div></body></html>";
```

To put cookies onto Safari, the ads on Google's network used something called an "iframe," an invisible container that allows content from one website to be embedded within another site, such as an ad on a blog. Through this "iframe" window, Google received data from the user's browser and was able to tell whether the person was using Safari.

```
<html>
<head></head>
<body>
<form id="drt_form" method=post action="/pagead/drt/si?p=CAA&amp;ut=AFAKxlQAAAAATzM2UG441tG4iy5pvhSs7gsiM952Odb-"></form>
```

If the person was using Safari, Google then inserted an invisible form into the container.

```
<script>
document.getElementById('drt_form').submit();
</script>
```

The user didn't see or fill out the form – in fact, there was nothing to "fill out" – but nevertheless, the Google code "submitted" it automatically. Once the form is sent, Safari behaves as though the user has filled something out intentionally, and the browser allows Google to store the cookie on the user's machine.

```
.doubleclick.net, _drt_, AFkicjf72GVnTzw5zsyQ2-mgP_RPRXmtJfgwXXt-jusrUMhAB-LYAGoMSXTBAuvEN-YDN3-Ggfmt9gxT62HNVuaucHGsjssv7A
```

If the person was logged in to Google Plus, the cookie would contain encoded information about that account.

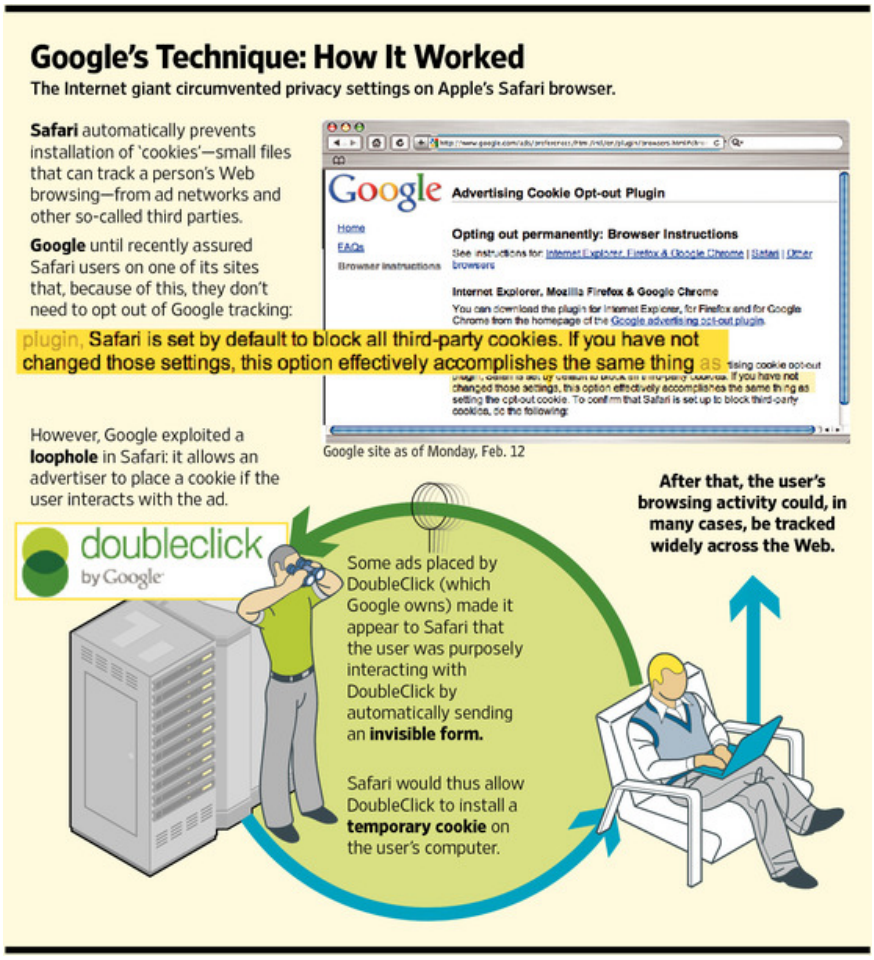
```
.doubleclick.net,_drt_,NO_DATA
```

If the person wasn't logged in, the cookie would still be placed on the computer, but it would be blank.

```
.doubleclick.net,id, 225f401f5201002e||t=1328801360|et=730|cs=002213fd4890910dc3faab6200
```

If a person received any of these cookies, which were temporary, other Google cookies could be added as soon as the user saw another Google ad. This included the DoubleClick ID cookie, the primary tracking cookie for Google's ad network.

Source: Jonathan Mayer and Ashkan Soltani. WSJ research



Google

79. Prior to the disclosure that Google was circumventing the Safari default third-party-cookie-blocking settings, Google hosted a webpage explaining to users how to effectively block advertising cookies, which conceded, "Safari is set by default to block all third-party cookies. If you have not changed those settings, this option essentially accomplishes the same thing as setting the opt-out cookie."[55] Google removed this misrepresentation from its website

[55] *Google Advertising Cookie Opt-out Plugin*, *available at* http://dl.dropbox.com/u/37533397/tracking_the_trackers/safari_study/google_safari_instructions.png.

after the details of Google's improper circumvention of Safari's default settings as described in this Complaint were exposed to the public.[56]

80. Moreover, Google's Privacy Policy in effect before the allegations that are the basis of this action became public, included the following, under the heading "Choices":

> "Most browsers are initially set up to accept cookies, but you can reset your browser to refuse all cookies or to indicate when a cookie is being sent. However, some Google features and services may not function properly if your cookies are disabled."[57]

81. The version of Google's Privacy Policy dated March 1, 2012, just a few weeks after Mr. Mayer's report became public, removed this language.[58]

82. Google's unofficial motto has long been "Don't Be Evil."[59] In various places throughout its website Google reiterates this affirmation to its users in various ways, such as that the motto is "built around the recognition that everything we do in connection with our work at Google will be, and should be, measured against the highest possible standards of ethical business conduct."[60]

83. The manner in which Google secretly, and without user consent, disabled the Safari browser's "no tracking" default position illustrates Google's knowing and intentional

---

[56] *See Consumer Watchdog letter to FTC Chairman Jon Leibowitz*, (Feb. 17, 2012), at 2 http://www.consumerwatchdog.org/resources/ltrleibowitz021712.pdf (comparing Google's pages before and after being confronted with the Mayer Study).

[57] *Google Privacy Policy*, (last modified Oct. 3, 2010, archived version), http://www.google.com/policies/privacy/archive/20101003/.

[58] *Google Privacy Policy, Comparison between March 1, 2012 and October 20, 2011 versions*, http://www.google.com/policies/privacy/archive/20111020-20120301/.

[59] *See, e.g.*, *Letter from the Founders, 'An Owner's Manual' for Google's Shareholders*, Google, Inc., SEC Form S-1, at 32, *available at* http://www.sec.gov/Archives/edgar/data/1288776/000119312504142742/ds1a.htm#toc59330_1.

[60] *See* Google's *Code of Conduct*, available at: http://investor.google.com/corporate/code-of-conduct.html; *see also* Item 6 in Google's *Ten Things We Know to be True*, http://www.google.com/about/company/philosophy/.

interception of and access to user information to which Google was not entitled and to which these users did not consent.

84. Google contracts with first-party websites for Google to provide display advertisements on those first-party webpages.[61] Those webpages, of content providers sometimes called "publishers," then provide Google an empty space within which Google can place the code Google uses to place individual ads.[62] Some publishers provided spaces called "iframes" for the Google-supplied ads.[63]

85. When a user types a content publisher's webpage address into the user's Safari navigation bar, the user's Safari browser starts by sending a GET request to the server which hosts the publisher's webpage. This GET request instructs the server to send all information for the publisher's webpage back to the user's browser for display on the monitor of the user's computing device.

86. In connection with this exchange of information, the server hosting the publisher's webpage also instructs the user's web browser to send a GET request to Google to

[61] Generically called "ad serving," the process is concisely described in a September 3, 2010 article *How Does Ad Serving Work* in AD OPS INSIDER, http://www.adopsinsider.com/ad-serving/how-does-ad-serving-work/. Describing what can be an eleven-step process requiring "mere milliseconds," or not "more than a second," this article delineates the interactions between users' browsers, the webpages they visit, and the advertising content supplied by ad serving computers to fill spaces for such advertising on the visited webpages.

[62] In or about June 2011 Google changed its policy from discouraging, to prohibiting, without Google's permission, web publishers' placement into an iframe of Google-supplied ads. *See* A. Agarwal, *You can No Longer Place Google Ads in an IFRAME*, www.labnol.org/internet/google-ads-in-iframe/19457/; P. Parker, *Google Bans iFrames for AdSense, Though Says It Will Grant Exceptions*, (June 10, 2011), http://searchengineland.com/google-bans-iframes-for-adsense-though-says-it-will-grant-exceptions-81174

[63] An "iframe" is a document within a document that, when a user requests information from a certain webpage, will, in turn, notify the iframe's creator that the user is requesting the "document within the document" for viewing.

display the relevant advertising information for the space on the page for which Google has agreed to sell display advertisements.

87. Upon the user's browser sending this GET request for the page on which the iframe is located, Google inserts code into the publisher's webpage that instructs the user's browser (1) to begin sending communications to the webpage http://google.com/pagead/drt/ui and (2) to automatically refresh itself after short intervals.

88. The webpage http://google.com/pagead/drt/ui responds to these communications differently depending on whether the user is logged-in to a separate Google account.

89. If the user is logged-in to a Google account, http://google.com/pagead/drt/ui responds by directing the user's browser to Google's authentication service to synchronize the ads with the particular user's personalized information and then directs the Safari browser to googleads.g.doubleclick.net for placement of the personalized advertisement. Google's documentation of this process suggests that the re-direct to googleads.g.doubleclick.net includes encrypted information on the user's account ID with Google, which includes personally identifiable information.

90. If the user is not logged-in, http://google.com/pagead/drt/ui directs the Safari browser straight to googleads.g.doubleclick.net. In a browser other than Safari, Google then sets a personalized cookie called "_drt_" on the user's computer through doubleclick.net.[64]

91. In Safari, however, the "_drt_" cookie is supposed to be blocked unless the user submits a form to doubleclick.net.

92. To avoid Safari's default settings which would block the placement of the "_drt_" cookie, Google sends back a page for Safari to place into the empty space or iframe which includes (1) an invisible form and (2) code which automatically submits the form back to Google's own webpage at doubleclick.net without the user taking any action.

[64] *DoubleClick is Google's digital advertising arm. See, e.g.,* http://www.google.com/doubleclick/.

93. The invisible form and the code accompanying it trick the user's browser into "requesting" the "_drt_" cookie from doubleclick.net without any action of the actual user.

94. Once the "_drt_" cookie is set through this invisible and fraudulent form submission, all other subsequent doubleclick.net cookies avoid blockage by Safari's default settings and are loaded onto the user's browser and device.

95. These other doubleclick.net cookies include one named "id," which is a unique and consistent identifier given to each user by Google for its use in tracking persons across the entire spectrum of websites on which Google places doubleclick.net cookies.

96. Google's website informs potential ad buyers that it can identify web users with Google's doubleclick.net cookies, "For itself, Google identifies users with cookies that belong to the doubleclick.net domain under which Google serves ads. For buyers, Google identifies users using a buyer-specific Google User ID which is an obfuscated version of the doubleclick.net cookie, derived from but not equal to that cookie."[65] As alleged in paragraph 466 above, the placement of the third-party cookies, placed by circumventing Plaintiffs' and Class Members' privacy settings, allows this identification to take place.

97. The Google cookies are then used to track and collect the Internet use and communications of the Plaintiffs and Class Members. In its Privacy Policy in effect when Google's secret circumvention of the Safari default setting was discovered, Google admitted that it does sometimes collect collected the actual *content* of user communications. In the "User communications" section of Google's disclosure of "Information we collect and how we use it," Google said in part: "When you send and receive SMS messages to or from one of our services that provides SMS functionality, we may collect and maintain information associated with those

[65] *DoubleClick Ad Exchange Real-Time Bidding Protocol, Background*, https://developers.google.com/ad-exchange/rtb/cookie-guide.

messages, such as the phone number, the wireless carrier associated with the phone number, the content of the message, and the date and time of the transaction."[66]

98. Google's cookies enabled Google to match up the user with a variety of additional substantive information about users' Internet use and communications if such information was collected in the past. This information includes, but is not limited to: information that users' provide,[67] including "personal information," which Google defines in its Privacy Policy as "information which you provide to us which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google."[68] This tracked and collected information also allows Google to obtain the following information, without limitation: home and business addresses; the URLs of each webpage the plaintiff requests and views; the time the plaintiffs visited such webpages; what the plaintiffs did on those webpages; the duration of the plaintiffs' visit to the webpage; the nature of the

[66] *Google Privacy Policy*, (last modified Oct. 3, 2010, archived version), http://www.google.com/policies/privacy/archive/20101003/.

[67] *See Id.* ("We may collect the following types of information" and describing the following sources of information: "information you provide;" "cookies;" "log information;" "user communications;" "affiliated Google Services on other sites;" "Third Party Applications;" "Location Data;" "Unique application number;" and "Other sites." Google then states: "In addition to the above, we may use the information we collect to: Provide, maintain, protect, and improve our services (including advertising services) and develop new services…." Google states that it "may combine the information [users] submit under [their] account[s] with information from other Google services or third parties in order to provide you with a better experience and to improve the quality of our services." Concerning tracking "cookies," Google's statements reveal that Google is obtaining specific data about users, because Google admittedly uses cookies for "improving search results and ad selection, and tracking user trends, such as how people search. Google also uses cookies in its advertising services to help advertisers and publishers serve and manage ads across the web and on Google services." Particularized, substantive content is necessary for these "services." Describing its "log information," Google discloses: "When you access Google services via a browser, application or other client our servers automatically record certain information. These server logs may include information such as your web request, your interaction with a service, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser or your account."

[68] *Google Privacy Policy, Key Terms*, http://www.google.com/policies/privacy/key-terms/.

plaintiffs' computing device, its browser type and operating system; the UDID of plaintiffs' mobile computing device; plaintiffs' IP addresses; additional GET requests and POST submissions from the plaintiffs; and whether they purchased goods and otherwise interacted with third party websites.

99. Google's DoubleClick affiliate also employed GIF tags that enabled the tracking of users' movements across websites associated with DoubleClick, learning what users wanted to see, what they looked at, and other information used for behavioral targeting.

100. Google's reason for hacking past the Safari browser's privacy setting was financial. Google's powerful and successful competitor, Facebook, had come up with the now ubiquitous "Like" button.

101. Google sought to compete with Facebook's "Like" button, so Google added a "+1" button to select Google ads. Google+[69] users could click that button to show they "liked" those ads.

102. But, Google ran into a big technical problem. Google was set up so that Google+ and Google Ads were on separate "domains." Interfacing between these two separate domains required use of third-party cookies. But, as described herein, Safari *blocked* those third-party cookies.

103. Google's problem was that most Safari users, a very big user constituency or, put otherwise, a large market base – would be unable to use Google's new "+1" feature. That would mean Google would lose advertising market share and precious revenue to competitors, especially Facebook. As Julia Angwin wrote in a March 16, 2012 *Wall Street Journal* article, "Advertisers will pay a premium for highly targeted ads, and Google is in a heated battle with social-networking rival Facebook, Inc. for these ad dollars."[70]

---

[69] Google+ is Google's social networking platform.

[70] Julia Angwin, *Google in New Privacy Probes*, WALL ST. J. (Mar. 16, 2012), *available at*, http://online.wsj.com/article/SB10001424052702304692804577283821586827892.html.

104. Unwilling to cede the field to Facebook and Facebook's Like button, Google came up with a way around this problem – the circumvention code uncovered by Jonathan Mayer as described herein.

105. Neatly summarizing Google's illegal solution, Brian Chen, in an article entitled *Google's Cookie Trick in Safari Stirs Debate* appearing in *Bits,* The New York Times blog covering "The Business of Technology," said: "Google's loophole involved tricking the Safari browser into allowing it to install cookies to serve ads with a tie-in to its Google Plus social network – adding a +1 button to ads for users to click if the user approved of them. Because of another quirk in Safari, this opened the door for additional Google cookies to be installed, potentially allowing wider tracking of users…."[71]

106. Google has never provided any explanation, or provided any facts, to show, or even to permit a reasonable inference, that Google's creation and use of the invisible form and embedded secret code were accidental.

107. Google has never provided any test data, analyses, studies or even theories supporting the claim that Google's hack of the Safari privacy setting was accidental.

108. Google has offered no facts, or reasons to believe, that Google would not have continued hacking around the Safari privacy default setting had Mr. Mayer and the *Wall Street Journal* not exposed Google's deception.

109. Google's systems received information from the secretly placed tracking cookies. Google monitors that information. Google received substantially more data than it would have absent the hack, because of Safari's market share. Google knew that it was getting information that the Safari browser was supposed to be blocking.

[71] Brian X. Chen, *Google's Cookie Trick in Safari Stirs Debate*, N.Y. TIMES BITS BLOG, (Feb. 17, 2012), http://bits.blogs.nytimes.com/2012/02/17/iphone-google-safari/.

110. According to the *Wall Street Journal* article reporting Mayer's discovery, Google added the secret computer code to certain of its online ads in 2011.[72] When revealed, Google's hack was neither recent nor temporary.

111. Google's secret code, which was embedded in certain ads that Google presented, contained instructions. Google personnel wrote those instructions. Those instructions permitted the "secret-code-disabling-Safari-privacy-followed-by-secret-tracking cookie" deception to work without the computer user knowing. Those instructions created a surrogate for user action.

112. When caught by Mr. Mayer, Google gave a number of explanations for its hack. One of them, from Rachel Whetstone, Google's Senior Vice President of Communications and Public Policy, was that Google "created a temporary communication link between Safari browsers and Google's servers, so that we could ascertain whether Safari users were also signed into Google, and had opted for this type of personalization."[73] But, as Mr. Mayer pointed out, the entire reason for checking to see if Google users were or were not logged in to Google was to link Google's general ad tracking cookie with the user's Google account, producing personally-identifiable, user-specific information.[74]

113. Google's after-the-fact justification that no personally identifiable data was collected is factually false, or, at best for Google, requires factual examination. As one commentator stated:

---

[72] Angwin & Valentino-Devries WSJ Article, http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html.

[73] *See* Shaun Nichols, *Google Accused of Tracking Safari Users*, SEARCH ENGINE WATCH (Feb. 20, 2012, http://searchenginewatch.com/article/2153478/Google-Accused-of-Tracking-Safari-Users (last visited Dec. 14, 2012).

[74] *See* Mayer Study. *See also* Doug Miller, *Safari-Gate: Did Google Break Government Computing Laws?* AOL GOV'T (May 10, 2012), http://gov.aol.com/2012/05/10/safari-gate-did-google-break-government-computing-laws/ ("Miller Article"); Jennifer Valentino-DeVries, *How Google Tracked Safari Users*, WALL ST. J. DIGITS BLOG (Feb. 16, 2012), http://blogs.wsj.com/digits/2012/02/16/how-google-tracked-safari-users/ ("Stanford's Mr. Mayer…said: 'There are zero legitimate-use cases' for advertisers to use an invisible form to enable tracking that Safari would have otherwise blocked.").

> Not only was Google installing cookies unbeknownst to users, but the tracking Google was able to do via these cookies was not anonymous if users were logged into a Google account….[F]or users logged into a Google account, the tracking was directly tied to their Google credentials. In [Jonathan] Mayer's words, "Identifying and identifiable information was collected. Google's social advertising technology is designed to identify the user."[75]

114. Google used an invisible code and an invisible space or web frame, to send an invisible form that mimicked a user's voluntary action, as one writer summarized it.[76]

115. Absent facts that Google has never disclosed, the known facts, and all reasonable inferences from those facts, show that Google's Safari hack was intentional.

116. In the nine months since Mr. Mayer revealed Google's Safari hack, Google has offered no facts showing, or plausibly suggesting, anything to refute Mr. Miller's conclusion:

> This was a deliberate, intentional, premeditated action to download and run an unauthorized hidden code in ads presented by Google … with the sole purpose of circumventing the security settings on Safari and enabling advertising features from which Google profited. As many have stated before, Google earns 96% of its revenue from advertising so it is logical that it would do whatever it could to optimize ad revenue potential on any user's Internet browsing sessions.[77]

117. Putting aside Google's failure to provide any facts tending to show the hack was accidental, or the work of an inept, misguided or rogue employee, common sense and experience compel the conclusion, and at minimum credibly raise the reasonable inference, that Google's Safari hack was intentional. Google's financial model depends on advertising revenue. Estimates vary, but it is safe to say over 95% of Google's revenues come from advertising. Google's "total advertising revenues" for the nine months ended September 30, 2012, which includes "Google websites" and "Google Network Members' Websites" was $31,610,000

[75] Miller Article.

[76] *Id.*

[77] *Id.*

against "other revenues" of $1,525,000, for a total advertising revenue percentage of total revenues of 95.4%.[78]

118. Tracking promotes Google's centrally important advertising revenues. Google's huge, successful competitor Facebook had implemented the popular "Like" button. Google needed its "+1" feature to make the "+1" feature work to personalize ads. Finally, as one commentator put it: "It is hard to imagine that a company as smart as Google could credibly not 'anticipate that this would happen.'"[79]

119. Upon being caught by Mr. Mayer, Google said it had "now started removing these advertising cookies from Safari browsers."[80]

120. To borrow from one blogger, Google used a code that "uses an invisible form to emulate Little Red Riding Hood and gain access to Grandma's house, exposing the user to whatever tracking Google Ads decides to subject Grandma."[81]

121. Google hacked around Safari's privacy setting block of third-party cookies to enable Google's "+1 Ads" feature to personalize ads, and to permit Google to collect more PII about users through Google's general tracking cookie, to advance Google's economic interest at the expense of the privacy and security interests of Google's users.

122. Mr. Mayer questioned Google's protestations that Google did not misuse any PII: "They were quite intentionally moving information about a Google user's account over to Google's advertising networks."[82]

---

[78] Google Inc. Form 10-Q for the quarterly period ended September 30, 2012, at 8.

[79] Miller Article.

[80] *Id.*

[81] Kristen Lovin, *Safarigate: Benign Behavior or Malignant Breach*, COLUM. SCI. & TECH. L. REV. (Feb. 22, 2012), http://www.stlr.org/2012/02/safarigate-benign.

[82] Stacy Cowley, *Google Caught Skirting Safari Privacy Settings*, CNNMONEY.COM (Feb. 17, 2012), http://money.cnn.com/2012/02/17/technology/google_tracking_safari/index.htm.

123. Mr. Mayer soon refined his February 17, 2012 analysis of Google's hack that undid Safari's default privacy settings. In a February 20, 2012 article, "Setting the Record Straight on Google Safari Tracking" on his blog,[83] responding to Google's explanation, Mr. Mayer began by "unpacking the four business practices that are at issue:"

a. **Social advertising.** Google is leveraging user account information to personalize its advertising on non-Google websites. To do that, Google now identifies its users when they view ads on non-Google websites.

b. **Social advertising circumvention.** Google intentionally bypassed Safari's cookie blocking feature to place an identifying cookie that it uses for social advertising.

c. **Ordinary advertising circumvention.** Google's social circumvention had a collateral effect: it enabled Google to place its ordinary advertising tracking cookie.

d. **Representation.** A Google instructional webpage claimed that Safari's cookie blocking feature 'effectively accomplishes the same thing' as opting out of Google's advertising cookies.

124. Refuting Defendants' claims that no individually identifiable information was collected, Mr. Mayer cited to the work of Arvind Narayanan showing that "third-party web tracking is in general not anonymous" and quoting Mr. Narayanan: "'There is no such thing as anonymous web tracking.'"[84] The same sort of sophisticated technology that enabled Google to hack the Safari default privacy setting enables Google and the other Defendants to connect the information they collect to specifically identifiable computer users in many cases.

---

[83] Jonathan Mayer, *Setting the Record Straight on Google's Safari Tracking*, WEB POLICY BLOG, (Feb. 20, 2012), http://webpolicy.org/2012/02/20/setting-the-record-straight-on-googles-safari-tracking/.

[84] Arvind Narayanan, *There is No Such Thing as Anonymous Online Tracking*, THE CENTER FOR INTERNET AND SOCIETY BLOG, (July 28, 2011), http://cyberlaw.stanford.edu/blog/2011/07/there-no-such-thing-anonymous-online-tracking ("Narayanan Article").

125. Google's surreptitious code was inserted into ads without the knowledge or consent of the owners of the webpages on which the ads were placed.

126. The following comments were made by spokespeople from websites on which Google ads appeared that used the surreptitious code described in this Complaint, without consent, in response to an article from the *Wall Street Journal* exposing the practice:[85]

- "We were not aware of this behavior. We would never condone it." Michael Balmoris, spokesman for AT&T, which owns YellowPages.com.
- "We didn't know about it and if accurate, we wouldn't be happy about it. Obviously, we're concerned about how it could negatively impact our users' experiences[.]" Craig Palmer, CEO of Wikia, the for-profit relative of Wikipedia which operates the website Wikia.com.
- "We've been using DoubleClick like thousands of other publishers have to serve ads, and were not aware of potential privacy issues. User privacy has always been of utmost importance to HubPages. As we learn more about this, we will ensure that our use of DoubleClick falls in line with our longstanding policy regarding user privacy." Paul Edmondson, CEO of HubPages.com.
- "This situation is nothing we are aware of." Photobucket.com.
- "We've told Google we don't support this activity." Seth Godin, spokesman for Squidoo.com.

PointRoll

127. PointRoll's use of its added codes also demonstrated that PointRoll intentionally and secretly disabled users' Safari browser default "do not track" settings to intercept and otherwise gain unauthorized access to users' information.

---

[85] *Comments From Companies Where Ads With Tracking Code Were Displayed*, WALL ST. J. (Feb. 16, 2012), http://online.wsj.com/article/SB10001424052970204880404577227931274732206.html.

128. When a user types the name of a webpage with PointRoll advertisements into their Safari navigation bar or clicks a link, their Safari browser starts by sending a GET request to that webpage instructing the server to send all information for that webpage back to the user's browser for display on the monitor of their computing device.

129. After this exchange of information, the server hosting the webpage also instructs the user's web browser to send a GET request to PointRoll to display the relevant information regarding PointRoll advertisements on the webpage for the user.

130. Upon the user's browser sending a GET request to PointRoll's server, PointRoll's server responds with code to create a new division on the webpage that includes an invisible iframe and form along with code, which automatically submits the form back to PointRoll's server without the user taking any action.

131. The invisible form and the code accompanying it force the user's browser into requesting cookies through a "Set-Cookie" header within the fraudulent form submission without the user taking any action.

132. With this invisible and fraudulent form submission, PointRoll has evaded Safari's default settings for its cookies.

133. PointRoll responds to this invisible and fraudulent form submission by setting nine cookies on the user's device.

134. One of the cookies set is named "PRID" – which, upon information and belief, is a unique ID cookie PointRoll creates to track persons across the entire spectrum of websites on which PointRoll places advertisements.

135. Safari's default settings and the potential for surreptitious code to trick the browser into setting third-party cookies was noticed by a blogger and developer named Anant Garg in 2010. On February 18, 2010, Garg published code to avoid "the problem" of Safari "not allow[ing]" third-party cookies.[86] Upon information and belief, PointRoll's code described

[86] Anant Garg, *Cross-domain Cookies/Sessions in Safari and All Other Browsers*, (Feb. 18,

herein was derived in large part from the code Garg posted to his blog in 2010. As pointed out by Mayer, PointRoll's code had the same structure, used the same variable names, attributes, attribute ordering, and coding style, and even had the same coding error as Garg's code.[87]

136. Upon Mr. Mayer's February 17, 2012 exposure of PointRoll's Safari hack, Point Roll's CEO, Rob Gatto, stated, in a cryptic and carefully worded message he posted the same day: "PointRoll does not currently employ the Safari technique outlined in the article. PointRoll conducted a limited test within the Safari browser to determine the effectiveness of our mobile ads. This test did not involve the collection, retention or resale of any specific user information. The limited test ended on February 8, 2012, and we made the decision not to employ this practice further."[88]

137. Mr. Gatto's statement admits PointRoll's Safari hack was intentional.

138. Stanford's Mr. Mayer had given Mr. Gatto no choice. Mr. Mayer had already demonstrated in his article why he concluded PointRoll's "cookie blocking circumvention was intentional," by comparing the code PointRoll used to existing code from web developer Anant Garg. Mr. Mayer demonstrated: (i) PointRoll's and Mr. Garg's codes or "scripts" were "structured in the same way;" (ii) "[b]oth use the variable sessionForm and the handler function submitSessionForm;" (iii) "[b]oth use the same attributes, attribute ordering, and coding style in their iframe and form elements…" and (iv) "if you're still unconvinced, here's the giveaway: the scripts have the same bug."[89]

139. PointRoll has never denied that PointRoll never informed users or sought permission before circumventing the Safari default cookie-blocking setting.

2010), http://anantgarg.com/2010/02/18/cross-domain-cookies-in-safari/.

[87] Mayer Study.

[88] Rob Gatto, *Information Regarding Wall Street Journal Article*, POINTROLL BLOG, (Feb. 17, 2012), http://blog.pointroll.com/news_and_press/information-regarding-wall-street-journal-article/.

[89] Mayer Study.

140. PointRoll has never explained why PointRoll had not informed users or sought permission before engaging in this secret trick.

141. PointRoll has never said users somehow consented to, or authorized, PointRoll's hack of the Safari privacy setting.

142. PointRoll has never explained why it did not disclose its supposedly innocuous Safari "limited test" until after Mr. Mayer and the *Wall Street Journal* had revealed that hack to the world.

143. PointRoll has never pointed to any facts, or even suggested they exist, showing that PointRoll had always intended to tell users about PointRoll's Safari hack, even before Mr. Mayer and the *Wall Street Journal* disclosed it.

144. PointRoll has never explained how PointRoll protected, or de-anonymized, "specific user information."

145. PointRoll has never stated that PointRoll did not collect, keep or sell aggregated user information that can be later linked to individual users. Much supposedly de-anonymized data is readily linkable to particular individual users. From the Narayanan Article: "If the mountain of deanonymization research that has accumulated in the last few years has shown us one thing, it is that the data itself can be deanonymized by correlating it to external information — specifically, facets of users' browsing history that … they occasionally choose to reveal publicly."[90]

Vibrant

146. Vibrant, like Google and PointRoll, also hacked around the Safari browser "no tracking" default setting. Supplying its clients' advertisements to third-party websites visited by users employing Safari web browsers, Vibrant secretly included computer code in certain of those advertisements. After the delivery of the client's advertisement containing the embedded computer code, the user's browser sent an invisible form through cyberspace back to Vibrant.

[90] http://cyberlaw.stanford.edu/blog/2011/07/there-no-such-thing-anonymous-online-tracking.

Unknown to and unwished for by the user, that involuntary transmittal of a form, triggered by advertisements Vibrant supplied, tricked Safari into thinking that its exception for form transmittals was engaged, resulting in disabling of Safari's "no tracking" protection.

147. Vibrant then implanted a tracking cookie, "VM_USR," on the unsuspecting user's computing device. Similar to the processes described for Google and PointRoll, once this third-party cookie was in place on Plaintiffs' and Class Members' browsers, Vibrant was able to intercept future communications in the same manner previously described.

148. Stanford's Mr. Mayer exposed Vibrant's hacking of the Safari browser on or about February 17, 2012.

149. Mr. Mayer's February 17, 2012 blog entry entitled "Safari Tracker" stated: "We found conclusive evidence that Vibrant deliberately circumvents Safari's third-party cookie blocking feature."[91]

150. Mr. Mayer's February 17, 2012 article goes on to describe precisely how Vibrant managed this trick. Summarizing what Mr. Mayer described in more detail as Vibrant's "circumvention technology:"

* Vibrant's main advertising script loads from http://answers.us.intellixt.com/intellixt/front.asp?ipid=31690. When the browser has a Safari User-Agent string and no Vibrant cookie, the script includes a Safari-specific code.
* The Safari-specific code executes, adding an invisible iframe to the page.
* The iframe contains a form and a body onload handler that submits the form.
* The response to the form contains no content and an instruction to set a Vibrant ID cookie.
* The result is the setting on the user's computing device of Vibrant's VM-USR cookie, which Mr. Mayer confirmed is "a Vibrant ID by checking the National Advertising Initiative's cookie status page."

[91] Mayer Study.

151. The February 17, 2012 article by Julia Angwin and Jennifer Valentino-Devries in the *Wall Street Journal* states that Vibrant admitted to intentionally hacking the Safari default setting. The article quotes a Vibrant spokesperson saying the hack was a "workaround" designed to "make Safari work like all the other browsers." The spokesman admitted Vibrant used the trick "for unique user identification."[92]

152. Vibrant has never said users either consented to, or somehow otherwise authorized, Vibrant's disabling of the Safari default privacy setting.

Media

153. Media used a similarly secret and technologically similar ruse as the other Defendants to beat the Safari privacy protection. As it sent its clients' advertisements to webpages requested by users making GET requests, Media included secret code, or, what Mr. Mayer described as "a script," in certain Media advertising. That secret script tricked the user's browser into sending an invisible form to Media, in turn deactivating Safari's privacy protection. Media then implanted an "id" cookie on the unknowing user's browser.

154. Summarizing Mr. Mayer's February 17, 2012 article's section on Media's hack, which concluded that Media's secret script "circumvents Safari's cookie blocking feature:"[93]

* Media's ad-embedded script creates an invisible iframe and form.

* That script then submits the form into the iframe during the onload handler to the iframe.

* In response to the form submission, Media sets cookies.

* Media sets an "id" cookie, that is the "ZAP ID cookie." "ZAP" stands for "Zeus Advertising Platform," which Mr. Mayer describes as "WPP's 'integrated advertising and analytics platform.'" Mr. Mayer's article cites a vendor report describing ZAP as "'one

[92] Angwin & Valentino-Devries WSJ Article, http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html.

[93] Mayer Study.

of the cornerstone products created by [Media],'" that "'collects and stores over 13 months of historical-user level data and draws from it to provide complex and robust analysis.'" Mr. Mayer's article cites that same vendor report as saying "With ZAP, '[Media] is currently tracking the effectiveness of every single advertising element within many live campaigns that reach hundreds of millions of unique users per month.'"

* Media also set the "OAX" cookie, WPP's ID cookie for "WPP's B3 advertising optimization and custom marketplace product."

* Mr. Mayer "verified that the [Media] script was a tracking cookie with MIG's NAI status indicator."

155. Noting caveats, Mr. Mayer analyzes the Media script to conclude: "[W]e believe it is reasonable to infer that [Media's] circumvention was intentional."

156. Media's "id" cookie is just that – an "I D" or "identification" cookie. Media uses the "id" cookie to facilitate tracking Internet users' behaviors. No accident, that tracking is exactly what Media's Mr. Lesser described as Media's core mission: "to build technology and leverage data to give agencies and advertisers access to the audiences they are trying to reach." Mr. Lesser said: "Data is at the core of all of our products."[94]

157. Media's former GM, Mr. Lesser, confirmed that Media is "very closely integrated with WPP's agencies and helps them make smarter media decisions on behalf of our clients…"[95] In other words, "we track user data, collect it, and use it to ensure we can tell clients how to target their ads to receptive audiences so the clients don't waste their money." The title of a recent article by Mr. Lesser, now CEO of another WPP company, the "audience buying company" XAXis, neatly captures the concept: "How to use Data to Deliver the Right Ad to the

[94] Brian Lesser, *WPP's Media Innovation Group GM Brian Lesser On DSPs, Holding Cos And Launching ZAP 3.0*, ADEXCHANGER (June 10, 2012), http://www.adexchanger.com/agencies/wpp-group-mig/.

[95] *Id.*

Right Person at the Right Time."[96] Mr. Lesser pithily describes the "best" way for advertisers to reach customers in today's cacophony of endless and myriad advertising messages: "Audience buying, where we leverage massive amounts of data to deliver the right ad, to the right person, at the right time….With audience buying … ads are delivered based on who the person is, based on anonymous profiles developed from online, offline, and propriety sources."

158. But what Mr. Lesser says are "anonymous profiles" are often *not* anonymous, and, are built from personal information taken from computer users without their consent, knowledge or compensation, as described in the Narayanan Article referenced above.

159. Media never issued any public statements providing any facts that would permit the inference, let alone the conclusion, that Media's hack of the Safari privacy setting was accidental or otherwise unintentional.

160. Media never made any statements saying that users consented to, or authorized, Media's secret negation of the Safari default third-party-cookie-blocking setting.

161. WPP, Media's owner, also used the same kind of trick. WPP's "OAX" cookies[97] also provide information about user identification. WPP, too, is in the business of ensuring advertising goes to specifically identified and carefully targeted potential customers. WPP collects and uses data, too, to make that business work. Users who frustrate WPP's desire for data portend economic harm for WPP, so WPP figured out how to hack around that frustration to keep the data-for-dollars stream flowing.

162. WPP has issued no public statements offering any facts that would permit the reasonable inference, let alone compel the conclusion, that WPP's hack of the Safari default

---

[96] Brian Lesser, *How to use Data to Deliver the Right Ad to the Right Person at the Right Time* ADAGE DIGITAL (July 3, 2012), http://adage.com/article/digitalnext/data-deliver-ad-person-time/235734/.

[97] *See* Jim Edwards, *Apple Users Claim WPP's Media Innovation Group Hacked Their Web Browsers*, BUSINESS INSIDER (July 9, 2012), http://www.businessinsider.com/apple-users-claim-wpps-media-innovation-group-hacked-their-web-browsers-2012-7. *See also* Mayer Study.

third-party-cookie-blocking privacy setting was innocent, an accident, or otherwise an unintended and unnoticed artifact of WPP's use of computers in serving its clients.

The FTC Investigation of Google

163. Neither accident, nor happenstance, Google's privacy violations here are part of a systemic business model that depends centrally on gathering reams of private data that informed users would not knowingly give up, at least not without payment.

164. On October 13, 2011, Defendant Google signed a consent order with the FTC to settle a previous privacy case. The case related to charges that Google used deceptive tactics and violated its own privacy promises to consumers when it launched its first social network, Google Buzz, in 2010, in violation of the FTC Act. The FTC complaint alleged that when Google launched Buzz through Google's web-based email service, Gmail, Google led users to believe that they could choose whether or not to join the network, even though the options for declining or leaving the social network were ineffective.

165. The settlement barred Google from future privacy misrepresentations, required Google to implement a comprehensive privacy program, and called for regular, independent privacy audits for the next 20 years.

166. On August 8, 2012, the Federal Trade Commission filed a complaint against Defendant Google for violating that 2011 consent decree under which Google agreed to "not misrepresent in any manner, expressly or by implication" its privacy policies, the purposes for which it collects and uses information, and "the extent to which consumers may exercise control over collection, use, or disclosure of covered information."[98]

[98] *In the Matter of Google, Inc.,* FTC File No. 102 3136 (3/30/11), Decision and Order, Docket No. C-4336, Issued Oct. 13, 2011, *available at* http://www.ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf.

167. The August 8, 2012 complaint is based on the same set of actions that form the factual basis for the causes of action stated herein on behalf of users of the Apple Safari web browser:

> According to the FTC's complaint, Google specifically told Safari users that because the Safari browser is set by default to block third-party cookies, as long as users do not change their browser settings, this setting "effectively accomplishes the same thing as [opting out of this particular Google advertising tracking cookie]." In addition, Google represented that it is a member of an industry group called the Network Advertising Initiative, which requires members to adhere to its self-regulatory code of conduct, including disclosure of their data collection and use practices.
>
> Despite these promises, the FTC charged that Google placed advertising tracking cookies on consumers' computers, in many cases by circumventing the Safari browser's default cookie-blocking setting. Google exploited an exception to the browser's default setting to place a temporary cookie from the DoubleClick domain. Because of the particular operation of the Safari browser, that initial temporary cookie opened the door to all cookies from the DoubleClick domain, including the Google advertising tracking cookie that Google had represented would be blocked from Safari browsers.[99]

168. Defendant Google and the FTC attempted to settle the complaint by Google agreeing to pay a fine of $22.5 million, the largest fine in the history of the FTC for violating an FTC order.[100]

169. FTC Commissioner J. Thomas Rosch filed a strong dissent to the settlement, objecting to the FTC allowing Google to settle the Complaint without admitting to underlying facts:

---

[99] *United States v. Google, Inc.*, 12-CV-04177, (N.D. Cal. Aug. 8, 2012), Complaint available at http://ftc.gov/os/caselist/c4336/120809googlecmptexhibits.pdf.

[100] *See* FTC Press Release, *Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser – Privacy Settlement is the Largest FTC Penalty Ever for Violation of a Commission Order* (Aug. 9, 2012), http://ftc.gov/opa/2012/08/google.shtm. *See also* [Proposed] Stipulated Order for Permanent Injunction and Civil Penalty Judgment, *available at* http://ftc.gov/os/caselist/c4336/120809googlestip.pdf.

I dissent from accepting this consent decree because it arguably cannot be concluded that the consent decree is in the public interest when it contains a denial of liability.

First, the Stipulated Order for Permanent Injunction and Civil Penalty Judgment provides that "Defendant denies any violation of the FTC Order, any and all liability for the claims set forth in the Complaint, and all material allegations of the Complaint save for those regarding jurisdiction and venue." Yet, at the very same time, the Commission supports a civil penalty of $22.5 million against Google for that very same conduct. Condoning a denial of liability in circumstances such as these is unprecedented.

Second, in the *Circa Direct* case, the Court ordered the Commission to explain why a consent decree was in the public interest when there was a denial of liability. Here, far from explaining why this settlement is in the public interest despite Google's denial of liability, the Commission merely asserts in its accompanying Reasons for Settlement that the "commission believes that the settlement by entry of the attached final order is justified and well within the public interest."

Third, this is not the first time the Commission has charged Google with engaging in deceptive conduct. This is Google's second bite at the apple. The Commission accuses it of violating the Google Buzz consent order by "misrepresent[ing] the extent to which users may exercise control over the collection or use of covered information" and accordingly, seeks civil penalties for those violations. In other words, the Commission charges Google with contempt. This scenario – violation of a consent order – makes the Commission's acceptance of Google's denial of liability all the more inexplicable.

Fourth, it may be asserted that a denial of liability is justified by the prospect of a $22.5 million civil penalty. But $22.5 million represents a *de minimis* amount of Google's profit or revenues. Beyond that, the Commission now has allowed liability to be denied not only in this matter but also in the *Facebook* settlement where Facebook simply promised to "go and sin no more" (unlike Google, Facebook was not previously under order). There is nothing to prevent future respondents with fewer resources than Google and with lower profiles than Google and Facebook from denying liability in the future too.

Fifth, it may also be asserted that a denial of liability is warranted here because Google is being sued for the same conduct in another forum. But, I see no reason why the more common "neither admits nor denies liability" language would not adequately protect Google from collateral estoppels in those lawsuits.

> For the foregoing reasons, I dissent from the Commission's decision to accept this consent decree.[101]

170. On August 21, 2012, Consumer Watchdog, a public interest organization dedicated to investigating, advocating, mobilizing, and litigating on behalf of American consumers filed a motion requesting leave to file an amicus curiae brief in opposition to the proposed settlement before United States District Court Judge Susan Illston of the Northern District of California.[102] On August 28, 2012, Judge Illston granted Consumer Watchdog's request. Judge Illston held a hearing in the matter on November 16, 2012, upholding the settlement of what is still the largest fine ever levied for violation of a Commission order.

Allegations as to Microsoft Internet Explorer Users

171. The Platform for Privacy Preferences, hereafter "P3P," provides a language and process that websites can use to post their privacy policies in a machine-readable form – that is, a form that can be processed by software such as web browsers. To comply fully with P3P, a website is required to post a full P3P policy, describing all of its privacy practices; a website may, optionally, post a "Compact Policy" describing its uses of browser cookies, though websites that use only the Compact Policy are not in full compliance with the P3P 1.0 specification.

172. Prior to P3P, a privacy-conscious Internet user who wanted to learn about website cookie practices had only one choice—to read the privacy policy of every website visited—and to do so often to account for updates.

173. This approach to managing cookies raised problems for users:

---

[101] Dissenting Statement of Commissioner J. Thomas Rosch, *United States v. Google Inc.*, (N.D. Cal.), *In the Matter of Google Inc.*, FTC Docket No. C-4336, Aug. 9, 2012, *available at* http://ftc.gov/os/caselist/c4336/120809googleroschstatement.pdf. *See also* Ed Felten, FTC Chief Technologist, *FTC Settles with Google over Cookie Control Override*, TECH@FTC BLOG (Aug. 9, 2012), http://techatftc.wordpress.com/2012/08/09/google/.

[102] *See* http://www.consumerwatchdog.org/resources/ftcgooglemotion082112.pdf.

a. It is effectively impossible for a user to take the time to read the privacy policy of every website visited;[103]

b. It is challenging for a user to try to interpret websites' privacy policies because, even among websites with substantially similar privacy practices, each website describes its practices in different ways and with varying levels of detail;

c. It is difficult for a user to determine which details of a website's privacy policy apply to which parts of the website, since a website's privacy practices may vary from page to page, such as a home page contrasted with a sign-in/registration page, or a check-out page following a purchase; and,

d. In order to read a website's privacy policy, the user typically must actually visit the website and receive whatever cookies the website delivers before having a chance to learn what the site's privacy practices are.

174. The advent of P3P helped address these issues, as follows:

a. P3P provided a common language and syntax that websites could use to provide machine-readable versions of their privacy policies, including cookie-specific Compact Policies.[104]

b. P3P privacy statements could be quickly read by the user's web browser each time the user directed the browser to access a web page;

c. P3P permitted websites to offer detailed privacy policies, tailored to the unique cookie practices of specific web pages within a website; and,

---

[103] *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: A J. OF LAW & POL'Y FOR THE INFO. SOC'Y 540 (2008), *available at* http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Cranor_Formatted_Final.pdf.

[104] *See* The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, W3C Recommendation, Apr. 16, 2002, http://www.w3.org/TR/P3P/.

d. P3P-enabled web browsers could automatically filter and restrict cookies based on the users' privacy settings (including default privacy settings), including discarding or downgrading cookies based on P3P compact policies.

175. P3P policies are written in code to be read by computer browsers, not real persons.

176. In 2001, Microsoft released version 6 of its Internet browser software, Internet Explorer ("IE6"), and included in it the capability to process websites' P3P Compact Policies. IE6 processed websites' Compact Policies automatically and, based on privacy settings that Microsoft set by default and that users could adjust, automatically allowed or restricted websites' storage of cookies on users' computers.

177. IE6 gave users the ability to have their computers automatically examine the abbreviated privacy information that websites choose to disclose in their Compact Policies. Subsequent versions of IE gave users the same or better capabilities. IE assessed websites' Compact Policies for users before the users even visited and acquired cookies from websites. In addition, in response to the users' privacy settings, IE could take certain actions in response to the P3P information it acquired – such as to accept, reject, or restrict the cookies that websites transmitted to users.

178. Compact Policies, such as those that IE enabled users to assess automatically through their web browser, are expressed as a series of codes, called "tokens," each of which represents a standardized privacy expression defined in the P3P specification. For example, in the following Compact Policy "DP= NOI DSP COR NID ADMa OPTa OUR NOR," the "NID" token means that no identified user information is collected by the web pages to which the Compact Policy applies or, if it is collected, it is anonymized in a way that cannot reasonably be reversed to reveal the user's identity; and the "OUR" token means that identified user information is shared only with an agent whose use of the information is restricted to the purposes stated by the website. Likewise, the other tokens have predetermined meanings.

179. Under IE's default privacy settings, a website's unsatisfactory P3P Compact Policy can lead to several consequences. IE allows or limits cookies in different ways depending on the statements in the Compact Policy and whether the web entity offering the policy is a first party (a website that the user explicitly chooses to visit) or a third party (such as entities that display advertisements on a first-party website), as described above. For example, if a first-party website's Compact Policy states that the website shares users' Personally Identifiable Information without user consent, IE downgrades the website's "persistent" cookie to a "session" cookie – i.e., one that expires at the end of the user's browser session.

180. By default, IE is set to block third-party cookies unless the site includes a P3P Compact Policy Statement, which (1) informs the IE browser how the third-party website will use the cookie, and (2) ensures the IE browser that the third-party cookie will not be used to track the user's Internet activity and communications.

181. Protocol 4.2 of the P3P creates a default rule of acceptability for tokens which are not recognizable: "If an unrecognized token appears in a compact policy, the compact policy has the same semantics as if that token was not present."[105]

182. Protocol 3.2.1 of the P3P prohibits false or misleading P3P statements: "In cases where the P3P vocabulary is not precise enough to describe a website's practices, sites should use the vocabulary terms that most closely match their practices and provider further explanation in the CONSEQUENCE field and/or their human-readable policy. However, policies MUST NOT make false or misleading statements."[106]

183. Google chooses not to comply with P3P requirements. However, instead of designing its webpages without any P3P statement at all, which Google knows would lead to the

[105] The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, W3C Recommendation, 4.2 Compact Policy Vocabulary, Apr. 16, 2002, http://www.w3.org/TR/P3P/#compact_policy_vocabulary.

[106] *Id.* at 3.2 Policies, http://www.w3.org/TR/P3P/#Policies.

blockage of third-party cookies under IE's default settings, Google places false P3P code into its pages as follows:

> CP="This is not a P3P policy! See http://support.google.com/accounts/bin/answer.py?hl=en&answer=151657 for more info."

184. Because P3P policies are designed to be read by computer browsers, not humans, Internet Explorer does not understand the meaning of the sentence, "This is not a P3P policy!" Instead of reading the sentence as an ordinary human would, Internet Explorer reads the sentence to state that the Google-affiliated website does have a P3P policy, but that it uses terms which IE does not understand – and is thus acceptable for the placing of third-party cookies. As a result, the above-detailed code tricks Internet Explorer into believing Google's doubleclick.net cookies are placed from a website which is P3P compliant.

185. The support page linked to by Google's invalid P3P policy states, "Some browsers require third-party cookies to use the P3P protocol to state their privacy practices. However, the P3P protocol was not designed with situations like these in mind. As a result, we've inserted a link into our cookies that directs users to a page where they can learn more about the privacy practices associated with these cookies."[107]

186. Google knows that:

a. P3P policies are not designed to be read by human users, but instead by browsers that do not understand common English;

b. Users rely on the browsers' settings to allow or disallow cookies that the user would find acceptable or unacceptable; and

[107] Google Support, P3P and Google's Cookies, http://support.google.com/accounts/bin/answer.py?hl=en&answer=151657.

c. The link inserted into Google cookies to direct users to a page where they can learn more about "privacy practices associated with these cookies" does not actually appear on any page a user might actually see.

187. On or about February 20, 2012, Microsoft conducted its own investigation as to Google's bypassing of privacy settings in browsers in order to determine if the same or similar behavior was affecting its Internet Explorer users as were affecting users of the Apple Safari browser. Microsoft's findings are as follows:

> When the IE team heard that Google had bypassed user privacy settings on Safari, we asked ourselves a simple question: is Google circumventing the privacy preferences of Internet Explorer users too? We've discovered the answer is yes: Google is employing similar methods to get around the default privacy protections in IE and track IE users with cookies…
>
> We've found that Google bypasses the P3P Privacy Protection feature in IE. The result is similar to the recent reports of Google's circumvention of privacy protections in Apple's Safari Web browser, even though the actual bypass mechanism Google uses is different.
>
> By default, IE blocks third-party cookies *unless* the site presents a P3P Compact Policy Statement indicating how the site will use the cookie and that the site's use does not include tracking the user. Google's P3P policy causes Internet Explorer to accept Google's cookies even though the policy does not state Google's intent.
>
> P3P, an official recommendation of the W3C Web standards body, is a Web technology that all browsers and sites can support. Sites use P3P to describe how they intend to use cookies and user information. By supporting P3P, browsers can block or allow cookies to honor user privacy preferences with respect to the site's stated intentions.
>
> Technically, Google utilizes a nuance in the P3P specification that has the effect of bypassing user preferences about cookies. The P3P specification (in an attempt to leave room for future advances in privacy policies) states that browsers should ignore any undefined policies they encounter. Google sends a P3P policy that fails to inform the browser about Google's use of cookies and user information. Google's P3P policy is actually a statement that it is not a P3P policy. It's intended for humans to read even though P3P policies are designed for browsers to "read."[108]

[108] IEBLOG, *Google Bypassing User Privacy Settings,* (Feb. 20, 2012),

188. Google has effectively admitted Microsoft's allegations. Rather than denying the allegations, Google publicly presented the non-legal defenses of (1) alleged difficulty with compliance and (2) "everybody's doing it."

189. In a direct response to Microsoft's blog post, Google Senior Vice President of Communications and Policy Rachel Whetstone stated:

> Microsoft uses a "self-declaration" protocol (known as "P3P") dating from 2002 under which Microsoft asks websites to represent their privacy practices in machine-readable form. It is well-known – including by Microsoft – that it is impractical to comply with Microsoft's request while providing modern web functionality. We have been open about our approach, as have many other websites. Today the Microsoft policy is widely non-operational. A 2010 research report indicated that over 11,000 websites were not issuing valid P3P policies as requested by Microsoft.[109]

190. Impracticality is not a valid legal defense to any cause-of-action set forth in this complaint. In addition, the P3P privacy protections Google has publicly stated are "impractical" are also used, on information and belief, by Google for its own advertising sites.

CLASS ACTION ALLEGATIONS

191. This is a class action pursuant to Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure on behalf of a Class of all persons in the United States of America who used the Apple Safari or Microsoft Internet Explorer web browsers and who visited a website from which doubleclick.net (Google's advertising serving service), PointRoll, Vibrant Media, Media Innovation Group, or WPP cookies were deployed as part of a scheme to circumvent the users' browsers' settings to block such cookies and which were thereby used to enable tracking of the

---

http://blogs.msdn.com/b/ie/archive/2012/02/20/google-bypassing-user-privacy-settings.aspx.

[109] *See* Donald Melanson, *Microsoft Finds Google Bypassed Internet Explorer's Privacy Settings Too, But It's Not Alone (Update: Google Responds)*, ENGADGET (Feb. 20, 2012), http://www.engadget.com/2012/02/20/microsoft-finds-google-bypassed-internet-explorers-privacy-sett/.

class members Internet communications without consent. The Class Period runs from the date Defendants began implementing these circumvention practices until the present (the "Class Period").

192. Excluded from the Class are Google, PointRoll, Vibrant, Media, WPP, and their officers, directors, employees, affiliates, legal representatives, predecessors, successors and assigns, and any entity in which any of them have a controlling interest, as well as all judicial officers assigned to this case and their immediate families.

193. The members of the Class are so numerous that joinder of all members is impracticable. Plaintiffs estimate that there are millions of Class members.

194. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. The questions of law and fact common to the Class include:

a. What was the extent of Defendants' business practice of circumventing Plaintiffs' and Class Members' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data?

b. What information did Defendants collect from their business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data, and what did they do with that information?

c. Did Defendants engage in a common business practice of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data provided to Plaintiffs and Class Members?

d. Did Defendants' business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, use, and remotely store users' data disclose, intercept, and transmit personal information?

e. Did Defendants devise and deploy a scheme or artifice to defraud or conceal from Plaintiffs and the Class Members Defendants' ability to, and practice of, circumventing users' Computing Device security settings to transmit, access, collect,

monitor, and remotely store users' data, for their own benefit, personal information, and tracking data from Plaintiffs' and the Class Members' personal Computing Devices via the ability to track their data on their Computing Devices?

f. Did Defendants engage in deceptive acts and practices in connection with their undisclosed and systemic practice of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data on Plaintiffs' and the Class Members' personal Computing Devices and using that data to track and profile Plaintiffs' and the Class Members' Internet activities and personal habits, proclivities, tendencies, and preferences for Defendants' use and benefit?

g. Did the implementation of Defendants' business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data violate the Computer Fraud and Abuse Act, 18 U.S.C. § 1030?

h. Did the implementation of Defendants' business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data violate the Wiretap Act portion of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510 *et seq.*?

i. Did the implementation of Defendants' business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data violate the Stored Communications Act portion of the ECPA, 18 U.S.C. § 2701 *et seq.*?

j. Did the implementation of Google's business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data violate California's Computer Crime Law, Penal Code § 502?

k. Did the implementation of Google's business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and

remotely store users' data violate the California Invasion of Privacy Act, Penal Code § 630 *et seq.*?

l. Did the implementation of Google's business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data violate the Consumers Legal Remedies Act, California Civil Code § 1750 *et seq.*?

m. Did the implementation of Google's business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data violate the Unfair Competition Law, California Business and Professions Code § 17200 *et seq.*?

n. Did the implementation of Defendants' business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data result in Unjust Enrichment?

o. Are any of the Defendants liable under a theory of aiding and abetting one or more of the remaining Defendants for violations of the statutes and laws listed herein?

p. Are any of the Defendants liable under a theory of civil conspiracy for violation of the statutes listed herein?

q. Did Defendants participate in and/or commit or are they responsible for violation of law(s) complained of herein?

r. Have Plaintiffs and Class Members sustained damages and/or loss as a result of Defendants' conduct, and, if so, what is the appropriate measure of damages and/or loss?

s. Are Plaintiffs and Class Members entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein?

t. Are Plaintiffs and Class Members entitled to punitive damages, and, if so, in what amount?

195. Plaintiffs' claims are typical of the claims of other Class Members, as all members of the Class were similarly affected by Defendants' wrongful conduct in violation of law as complained of herein.

196. Plaintiffs will fairly and adequately protect the interests of the members of the Class and have retained counsel that are competent and experienced in class action litigation. Plaintiffs have no interests that are in conflict with, or otherwise antagonistic to, the interests of the other Class Members.

197. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages individual Class Members have suffered may be small compared to the cost of litigating their own cases, the expense and burden of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in management of this action as a class action.

COUNT I

VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA), 18 U.S.C. § 2510, *et seq.* AGAINST ALL DEFENDANTS

198. Plaintiffs incorporate by reference and re-allege all paragraphs previously alleged herein.

199. As described herein, Defendants intentionally intercepted Plaintiffs' and Class Members' electronic communications by conducting third-party tracking despite the fact that Plaintiffs Class Members were using their Safari and/or Internet Explorer browsers set to block such interceptions through third-party tracking.

200. Defendants intercepted Plaintiffs' and Class Members' electronic communications because, as described herein, they acquired the substance, purport, meaning or contents of those communications through the use of an electronic, mechanical or other device

when Defendants enabled third-party tracking in direct violation of the browser settings.

201. To intercept the contents of the electronic communications transmitted while Plaintiffs and Class Members used the Safari browser, Defendants made use of special software code specifically designed to circumvent the no-third-party-tracking setting. As described above, Defendants' software codes sent invisible forms, purportedly but not actually from the Plaintiffs and Class Members, to trick the Safari browser into permitting Defendants to place third-party tracking cookies. The special software codes disabled the Safari browser's blocking of third-party cookies, so that the Defendants could place additional third-party cookies (without facing further blocking by Safari) and conduct third-party tracking without Plaintiffs' and Class Members' consent. Defendants used the special unblocking software codes, with their invisible form that falsely appeared to be sent by the Plaintiffs and Class Members, as devices to enable their third-party cookies and their tracking systems to intercept the Plaintiffs' and Class Members' electronic communications without consent.

202. As described above, Google circumvented Internet Explorer's privacy settings, using as a device its false P3P code which, instead of providing machine-readable code that would truthfully communicate Google's practice of using third-party cookies to track users' web-browsing activities, instead used only human-readable code that improperly lead Internet Explorer to permit Google to install third-party cookies, even on the Computing Devices of those Plaintiffs and Class Members whose Internet Explorer was set to deny third-party tracking cookies. Google used the unreadable-to-Internet Explorer P3P code as a device that falsely appeared to indicate that Google did not use third-party cookies to enable its tracking systems to intercept the Plaintiffs' and Class Members' electronic communications without their consent.

203. Defendants used the devices described above to install third-party tracking

cookies that enabled Defendants to conduct third-party tracking of Plaintiffs and Class Members that constituted the acquisition of the contents of Plaintiffs' and Class Members' electronic communications. Those communications derived from the web browsing activities that their Safari and Internet Explorers facilitated and that the Defendants' third-party cookies tracked after deliberately bypassing and effectively disabling the tracking blocks. Much of the Class Members' web browsing activities constituted electronic communications under 18 U.S.C. § 2510(12), because they were the transfers of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affect interstate or foreign commerce.

204. As described above, none of the Defendants has offered a single credible fact suggesting their interceptions of Plaintiffs' and Class Members' electronic communications, accomplished by use of devices to circumvent the browsers' third-party tracking blocks and then by engaging in unconsented to and undisclosed third-party tracking, was accidental rather than intentional. Google, PointRoll, and Vibrant have all actually admitted to the conduct just described.

205. As described above, the Defendants' third party web tracking permitted them to uniquely associate with their third-party cookies detailed information about what websites a Plaintiff or Class Member visited, how long she spent there, what she looked at while she was there, what information she exchanged with the site, and what information she had exchanged with the site she had just visited prior to arriving at that site. When Defendants acquired web browsing information that specifically indicated the Uniform Resource Locators (URL's) that Plaintiffs and Class Members requested from the first party websites they were visiting, they acquired the contents of Plaintiffs' and Class Members' electronic communications because, by

identifying the specific page that a Plaintiff or Class Member viewed, URL's include information concerning the substance, purport or meaning of that communication under 18 U.S.C. § 2510(8). URL's, which third-party tracking records and stores, can identify specific items, such as websites, videos, pictures, or articles that a Plaintiff or Class Member chooses to look at, which are the substance of the communication.

206. As also described above, the Defendants' third-party web tracking permitted them to record information that Class Members exchanged with first-party websites during the course of filling out forms or conducting searches. Such information certainly constitutes the substance, purport or meaning of the Class Members' electronic communications with first-party websites, which Defendants' intercepted while not a party to those communications (hence third party tracking) and despite the fact that Class Members' browsers were set specifically to preclude the use of third-party cookies to track their behavior and record their electronic communications without their knowledge or consent.

207. For example, a Plaintiff's request for delivery of a first-party website's webpage to Plaintiff's Computing Device is itself substantive information. Defendants obtained not just the fact of a request but the exact request itself, which, because it includes URL information, is substantive. A GET request for www.helpfordrunks.com with further information about where to find AA meetings in Wilmington is substantive content of an intercepted communication.

208. As described above, Defendants' intercepted Class Members electronic communications contemporaneously with the transmission of those communications; in other words the Defendants' third-party tracking intercepted the Class members' communications while they were in transit from the Class Members' Computing Devices to the web servers of the first party websites the Class Members used their browsers to visit. In particular, during the

course of populating the advertising space on the first party website the Class Member had intended to visit, the Defendants' transmitted copies of the Class Members' communications to their own webservers as part of third party tracking to which the plaintiffs had not consented nor been made aware of. Separate, but simultaneous and identical, communications satisfy even the strictest real time interception requirement.

209. Upon information and belief, Defendants were able to associate information they obtained through the unconsented to and undisclosed third-party cookies described herein with the actual names and other personally identifying information of Plaintiffs and Class Members.

210. Upon information and belief, the first party websites, the communications with which were the subject of interception by the Defendants, did not consent to use of third party tracking by the Defendants.

211. As a direct and proximate result of such unlawful conduct, Defendants violated 18 U.S.C. § 2511 in that Defendants:

a. Intentionally intercepted, endeavored to intercept, or procured another person to intercept or endeavor to intercept Plaintiffs' and Class Members' electronic communications;

b. Upon belief predicated upon further discovery, under Federal Rule Civil Procedure 11(b)(3), intentionally disclosed or endeavored to disclose to any other person the contents of Plaintiffs' and Class Members' electronic communications, knowing or having reason to know that the information was obtained through the interception of electronic communications in violation of 18 U.S.C. § 2511(1)(a).

c. Upon belief predicated upon further discovery, under Federal Rule Civil Procedure 11(b)(3), intentionally used or endeavored to use the contents of Plaintiffs' and

Class Members' electronic communications, knowing or having reason to know that the information was obtained through the interception of electronic communications in violation of 18 U.S.C. § 2511(1)(a).

212. As a result of the above violations and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages to Plaintiffs and the Class in the sum of the greater of $100 for each day a Class Member's electronic communications were intercepted, disclosed or used, or $10,000 per violation; injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendants in the future, and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT II

VIOLATION OF THE STORED COMMUNICATIONS ACT, 18 U.S.C. § 2701, *et seq*. ("SCA") AGAINST ALL DEFENDANTS

213. Plaintiffs incorporate by reference and re-allege all paragraphs previously alleged herein.

214. The Stored Communications Act ("SCA") provides a cause of action against a person who "intentionally accesses without authorization a facility through which an electronic communication service is provided," "or who intentionally exceeds an authorization to access that facility; and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage in such a system." 18 U.S.C. § 2701(a).

215. The statute defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof;" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

216. Defendants intentionally accessed without authorization or intentionally exceeded authorization to access facilities though which electronic communications systems were provided when they used the devices described herein to circumvent the browsers' blocks on third-party cookies and tracking. Apple Safari and Microsoft Internet Explorer both provide electronic communications service because they "provide to users thereof the ability to send or receive wire or electronic communications," 18 U.S.C. § 2510(15).

217. As described above, Safari and Internet Explorer both store cookie and other information in browser-managed files on the Plaintiffs' and Class Members' Computing Devices. Those browser-managed files are facilities under the SCA, and Defendants' intentionally accessed them without authorization or intentionally exceeded authorized access to them when they tricked the browsers into permitting them to place cookies in the browser-managed files on Plaintiffs' and Class Members' Computing Devices. Had the Plaintiffs and Class Members set the browsers to permit third-party cookies and tracking, access to those files, or facilities, would have been authorized under 18 U.S.C. § 2701(c)(1). Instead, the Defendants' obtained access through deceit, without the authorization either of the Plaintiffs and Class Members or the browsers themselves.

218. As described above, the cookies in the browser-managed files that Safari and Internet Explorer store on the Plaintiffs' and Class Members' Computer Devices, or facilities, are updated regularly to record users' browsing activities as they happen. For that reason, when the Defendants used their access to the facilities to acquire Class Members' electronic communications, they acquired both recently updated cookies and related just-transmitted electronic communications out of random access memory ("RAM"). The Defendants acquired

those cookies and related electronic communications out of electronic storage, incidental to the transmission thereof.

219. Plaintiffs and Class Members were harmed by Defendants' violations, and pursuant to 18 U.S.C. § 2707(c), are entitled to actual damages including profits earned by Defendants attributable to the violations or statutory minimum damages of $1,000 per person, punitive damages, costs and reasonable attorney fees.

COUNT III

VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030 ("CFAA") AGAINST ALL DEFENDANTS

220. Plaintiffs incorporate by reference and re-allege all paragraphs previously alleged herein.

221. Plaintiffs' and Class Members' Computing Devices were used in interstate commerce or communication. Plaintiffs' Internet browsing, which the Defendants impermissibly tracked, involved submissions to websites for companies all over the United States and the world, both for purchases of goods and for information.

222. The browser-managed files which Defendants' intentionally accessed without authorization or intentionally exceeded authorized access to when they tricked the browsers into permitting them to place and also access third-party cookies, as described above, were stored on Plaintiffs' and Class Members' Computing Devices.

223. Plaintiffs' and Class Members' Computing Devices are protected computers, as defined in 18 U.S.C. § 1030(e)(2).

224. Defendants intentionally accessed Plaintiffs' and Class Members' computers without authorization or exceeded authorized access to such computers, thereby obtained information from them, such as third-party cookie data stored there, in violation of 18 U.S.C. § 1030(a)(2)(c).

225. Defendants knowingly caused the transmission of a program, information, code or command and as a result intentionally caused a loss to Plaintiffs and Class Members during a one-year period aggregating at least $5,000 in value, in violation of 18 U.S.C. § 1030(a)(5)(a)(i).

226. Defendants intentionally accessed Plaintiffs' and Class Members computers without authorization or exceeded authorized access and as a result caused a loss to Plaintiffs and Class Members during a one-year period aggregating at least $5,000 in value, in violation of 18 U.S.C. § 1030(a)(5)(a)(iii).

227. Defendants' unlawful access to Plaintiffs' and Class Members' computers and communications have caused irreparable injury. Unless restrained and enjoined, Defendants may continue to commit such acts. Plaintiffs' and Class Members' remedies at law are not adequate to compensate for these inflicted and threatened injuries, entitling Plaintiffs and the Class to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

COUNT IV

INVASION OF PRIVACY AGAINST DEFENDANT GOOGLE

228. Plaintiffs incorporate by reference and re-allege all paragraphs previously alleged herein.

229. Google's Terms of Service in effect while Google was secretly circumventing the Safari default setting provide that California law governed the users' relationship with Google. Section 20.7 provided, in pertinent part: "The Terms, and your relationship with Google under the Terms, shall be governed by the laws of the State of California without regard to its conflict of laws provisions…."[110]

230. Plaintiffs and Class Members had an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential Personally Identifiable Information; and (2) making

[110] *Google's Terms of Service*, (April 16, 2007), http://www.google.com/policies/terms/archive/20070416/.

personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various Internet sites without having that information intercepted and transmitted to Google or other persons or entities without Plaintiffs' and Class Members' knowledge or consent.

231. Based on, among other things, privacy settings on their Internet browsers, Plaintiffs and Class Members had a reasonable expectation that their Personally Identifiable Information and other data would remain confidential and that Google would not install cookies on their browsers that would enable Google to obtain information about their Internet usage.

232. This invasion of privacy is sufficiently serious in nature, scope and impact.

233. This invasion of privacy constitutes an egregious breach of the social norms underlying the privacy right.

COUNT V

INTRUSION UPON SECLUSION AGAINST DEFENDANT GOOGLE

234. Plaintiffs incorporate by reference and re-allege all paragraphs previously alleged herein.

235. By sneaking around privacy settings on Plaintiffs' and Class Members' web browsers through invisible forms, invisible iframes and invisible embedded codes that produced invisible and unconsented-to tracking cookies used to intercept Plaintiffs' and Class Members' electronic communications on the Internet, Google intentionally intruded upon their solitude or seclusion.

236. Plaintiffs and Class Members did not consent to, authorize, or know about Google's intrusion until on or about February 17, 2012.

237. Under the applicable California law, Google's intentional intrusion on Plaintiffs' and Class Members' solitude or seclusion without consent would be highly offensive to a reasonable person. Google assured Plaintiffs and Class Members that if they were using the Safari browser devices, they needed to do nothing more to protect themselves from unwanted Google tracking of their web comings and goings. Google made that assurance at the same time

Google was, as Mr. Mayer concluded and the facts demonstrate, intentionally disabling the very privacy setting on which Google assured the Plaintiffs and Class Members they could rely. Google's deception was deliberate.

COUNT VI

VIOLATION OF CALIFORNIA BUSINESS AND PROFESSIONS CODE § 17200, *et seq*., THE UNFAIR COMPETITION LAW ("UCL") AGAINST DEFENDANT GOOGLE

238. Plaintiffs incorporate by reference and re-allege all paragraphs previously and subsequently alleged herein.

239. In violation of California Business and Professions Code § 17200, *et seq*. ("UCL"), Google's conduct in this regard is ongoing and includes, but is not limited to, statements made by Google about how, where and when Google placed cookies on Plaintiffs' and Class Members' Computing Devices.

240. By engaging in the acts and practices described herein, Google committed one or more acts of unfair competition within the meaning of the UCL, and as a result, Plaintiffs and the Class Members have suffered injury-in-fact and have lost money and/or property, namely, as described herein, the insertion of cookies on their computers, the collection and commercial use of their personal information, the invasion of their privacy and the lost value of their personally identifiable information and other data, that, as has been alleged herein, is a marketable commodity.

241. Under the UCL, Plaintiffs' loss of money or property need not be alleged in a particular dollar amount. Plaintiffs' UCL claims of economic loss can take innumerable legally cognizable forms.

242. Among other losses, Plaintiffs and Class Members gave up more personal information in their dealings with Google than they would have had Google disclosed its circumvention of Plaintiffs' and Class Members' Safari and Internet Explorer privacy settings.

243. Plaintiffs and Class Members received less privacy from Google than promised them, which is cognizable loss under the UCL.

244. Plaintiffs and Class Members lost the opportunity to sell the personal information at full value, because Google had already taken it without compensation, notice, or consent, diminishing its economic value to Plaintiffs and Class Members.

245. Google's business acts and practices are unlawful because, as alleged herein, they violate the California Consumers Legal Remedies Act, California Civil Code § 1750, *et seq*., California Penal Code § 502, California Penal Code § 630, *et seq.*, 18 U.S.C. § 2510, *et seq*., and 18 U.S.C. § 1030. Google is therefore in violation of the "unlawful" prong of the UCL.

246. Google's business acts and practices of circumventing Plaintiffs' and Class Members' web browser settings to place cookies are unfair, because they contradict federal and state constitutional and statutory privacy principles and cause harm and injury-in-fact to Plaintiffs and Class Members, and for which Google has no justification other than to increase, beyond what Google would have otherwise realized, Google's profits in fees from advertisers, software developers and other third parties, and the value of Google's information assets, through the acquisition of consumers' Personally Identifiable Information. Google's conduct lacks reasonable and legitimate justification in that Google has benefited from such conduct and practices while Plaintiffs and Class Members have suffered injury to their interests in the value, privacy and confidentiality of their Personally Identifiable Information. Google's conduct offends public policy in California as embodied in the Consumers Legal Remedies Act, the state constitutional right of privacy, and California statutes recognizing the need for consumers to obtain material information that enables them to safeguard their own privacy interests, including Cal. Civ. Code § 1798.80.

247. Moreover, Google knew, or should have known, that Plaintiffs and Class Members care about the confidentiality and privacy of their Personally Identifiable Information and Internet privacy and security, but Plaintiffs and Class Members were unlikely to be aware of the manner in which Google was engaged in practices that expressly violated Plaintiffs' and

Class Members' browser settings and Google's own representations. Google therefore violated the "unfair" prong of the UCL.

248. Google's acts and practices were fraudulent within the meaning of the UCL, because they were likely to, and did, in fact, mislead the members of the public to whom they were directed. For example, Google's website stated that "Safari is set by default to block all third-party cookies. If you have not changed those settings, this option essentially accomplishes the same thing as setting the opt-out cookie." However, as Plaintiffs have alleged in detail, Google performed a number of steps to circumvent the Safari settings, and did not permit Safari to carry out the same third-party cookie blocking that would accomplish the same thing as setting the opt-out cookie.

249. In reasonable reliance on Google's misrepresentations and omissions, Plaintiffs interacted with various websites believing that this information was secure and confidential. In actuality, without Plaintiffs' knowledge or consent, Google caused certain cookies to be placed on Plaintiffs' computers, which enabled Google to actively intercept and collect Plaintiffs' personally identifiable information so that it could be utilized for advertising and other purposes for Google's benefit.

250. Plaintiffs, on behalf of themselves and each Class Member, seek restitution, injunctive relief, and other relief as provided under the UCL.

COUNT VII

VIOLATIONS OF CALIFORNIA PENAL CODE § 502 THE CALIFORNIA COMPUTER CRIME LAW ("CCCL") AGAINST DEFENDANT GOOGLE

251. Plaintiffs incorporate by reference and re-allege all paragraphs previously alleged herein.

252. Cal. Penal Code § 502 is often described as an anti-hacking statute, aimed at prohibiting exactly the kind of clandestine, unconsented-to and otherwise unauthorized access to computing devices that Google obtained here.

253. Google violated Cal. Penal Code § 502(c)(2) by tampering and interfering with, and obtaining unauthorized access to, Plaintiffs' and Class Members' Computing Devices through the use of the secret embedded code that disabled the Safari browser privacy default setting and then knowingly and without permission accessing, taking and using Plaintiffs' and the Class Members' Personally Identifiable Information.

254. Google accessed and made use of data belonging to Plaintiffs and Class Members: (1) in and from the State of California; (2) in the states in which the Plaintiffs and the Class Members are domiciled; and (3) in the states in which the servers that provided services and communication links between Plaintiffs and the Class Members and Google and other websites with which they interacted were located.

255. Cal. Penal Code § 502 provides: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction."

256. Google violated California Penal Code § 502(c)(1) by knowingly accessing and without permission altering, damaging, and making use of Plaintiffs' and Class Members' Computing Devices in its circumventing of Plaintiffs' and Class Members' browser settings to place tracking cookies on Plaintiffs' and Class Members' Computing Devices in order to execute a scheme to defraud and deceive consumers by utilizing and profiting from the sale of their Personally Identifiable Information, thereby diminishing the value of their Personally Identifiable Information.

257. Google violated California Penal Code § 502(c)(2) by knowingly accessing and without permission taking and making use of Plaintiffs' and Class Members' Personally

Identifiable Information from their Computing Devices when Google circumvented Plaintiffs' and Class Members' browser settings to place tracking cookies on Plaintiffs' and Class Members' Computing Devices.

258. Google violated California Penal Code § 502(c)(6) by knowingly and without permission providing, or assisting in providing, a means of accessing Plaintiffs' and Class Members' Computing Devices when Defendants circumvented Plaintiffs' and Class Members' browser settings to place tracking cookies on Plaintiffs' and Class Members' Computing Devices to allow for the tracking of Personally Identifiable Information and electronic communications.

259. Google violated California Penal Code § 502(c)(7) by knowingly and without permission accessing, or causing to be accessed, Plaintiffs' and Class Members' Computing Devices when Google circumvented Plaintiffs' and Class Members' browser settings to place tracking cookies on Plaintiffs' and Class Members' Computing Devices to allow for the tracking of Personally Identifiable Information and electronic communications.

260. Pursuant to California Penal Code § 502(b)(10) a "Computer contaminant" is defined as "any set of computer instructions that are designed to ... record, or transmit information within computer, computer system, or computer network without the intent or permission of the owner of the information."

261. Google violated California Penal Code § 502(c)(8) by knowingly and without permission introducing a computer contaminant into the transactions between Plaintiffs and the Class Members and websites; specifically, a third-party tracking cookie that is used to enable the interception and gathering of information concerning Plaintiffs' and the Class Members' interactions with certain websites, which information is then transmitted back to Google.

262. As a direct and proximate result of Google's unlawful conduct within the meaning of California Penal Code § 502, Google caused loss to Plaintiffs and the Class Members in an amount to be proven at trial. Plaintiffs and the Class Members are also entitled to recover their reasonable attorneys' fees pursuant to California Penal Code § 502(e).

263. Plaintiffs and the Class Members seek compensatory damages, in an amount to be

proven at trial, and injunctive or other equitable relief.

264. Plaintiffs and the Class Members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Google's violations were willful and, upon information and belief, Google is guilty of oppression, fraud, or malice as defined in Cal. Civ. Code § 3294.

COUNT VIII

VIOLATIONS OF CALIFORNIA PENAL CODE § 630, *et seq.* THE INVASION OF PRIVACY ACT AGAINST DEFENDANT GOOGLE

265. Plaintiffs incorporate by reference and re-allege all paragraphs previously alleged herein.

266. California Penal Code § 631(a) provides, in pertinent part:

> Any person who … willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars…

267. At all relevant times, Google's secret circumvention of Plaintiffs' and Class Members' browser settings to place tracking cookies on Plaintiffs' and Class Members' Computing Devices that were used to access, intercept and collect Plaintiffs' and Class Members' Personally Identifiable Information, including their web browsing activity while Plaintiffs' and Class Members' browsers were set to block such cookies, was without authorization and consent.

268. Plaintiffs and Class Members, during one or more of their interactions on the Internet during the Class Period, communicated with one or more entities based in California, or with one or more entities whose servers were located in California, including TMZ.com.

269. Communications from the California web-based entities to Plaintiffs and Class Members were sent from California. Communications to the California web-based entities from Plaintiffs and Class Members were sent to California.

270. Plaintiffs and Class Members did not consent to any of Google's actions in intercepting and learning the contents of their communications with such California-based entities.

271. Plaintiffs and Class Members did not consent to any of Google's actions in using the contents of their communications with such California-based entities.

272. Plaintiffs and Class Members have suffered loss by reason of these violations, including, but not limited to, violation of the right of privacy and loss of value in their Personally Identifiable Information.

273. Unless restrained and enjoined, Google will continue to commit such illegal acts.

274. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and the Class have been injured by the violations of Cal. Penal Code § 631, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

COUNT IX

VIOLATIONS OF CALIFORNIA CIVIL CODE § 1750 THE CONSUMERS LEGAL REMEDIES ACT ("CLRA") AGAINST DEFENDANT GOOGLE

275. Plaintiffs incorporate by reference and re-allege all paragraphs previously alleged herein.

276. In violation of California Civil Code § 1750, *et seq*. (the "CLRA"), Google engaged and is engaged in unfair and deceptive acts and practices in the course of Google's interactions with Plaintiffs and Class Members.

277. At all relevant times, Plaintiffs and each proposed Class Member was a "consumer," as that term is defined in Cal. Civ. Code § 1761(d), because Plaintiffs and Class

Members exchanged their valuable personal information, as described above, for the acquisition of Google's goods and services, including search capacity and advertising, for personal, family and household purposes.

278. At all relevant times, Google's online services, including the provision of search capacity and advertisements to Plaintiffs and Class Members, constituted "goods" and "services," as those terms are defined in Cal. Civ. Code § 1761(b).

279. At all relevant times, Google was a "person," as that term is defined in Civ. Code § 1761(c), because Google is a corporation.

280. At all relevant times, Plaintiffs' and each proposed Class Member's use of websites within which Google supplied and placed advertisements and correspondingly implemented cookies as described above constituted a "transaction," as that term is defined in Civ. Code § 1761(e).

281. Google's practices, acts, policies, and courses of conduct violated the CLRA in that Google represented that its website and online services have characteristics, uses and benefits which they do not have, in violation of § 1770(a)(5) of the CLRA.

282. As previously described in detail, Google represented that it would supply its goods and services to Plaintiffs and Class Members in accordance with a previous representation and then did not, in violation of § 1770(a)(16). Google's website stated that "Safari is set by default to block all third-party cookies. If you have not changed those settings, this option essentially accomplishes the same thing as setting the opt-out cookie," However, as Plaintiffs have alleged in detail, Google took actions that circumvented the Safari settings, and did not permit Safari to carry out the same third-party cookie blocking that would accomplish the same thing as setting the opt-out cookie.

283. Plaintiffs and the Class suffered the aforementioned damages as a result of Google's conduct. On February 23, 2012, Lourdes Villegas provided Google with written notice of her and the Class's claims, via U.S. certified mail, return receipt requested, and demanded that within 30 days, Google correct, repair, replace or otherwise rectify the unfair and deceptive

practices complained of in her complaint for the entire Class, pursuant to Civil Code section 1770. Google failed to do so or agree to do so. Therefore, Plaintiffs now seek damages for such unfair and deceptive practices pursuant to Civil Code section 1782.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

A. Certify this action is a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure and appoint Plaintiffs as the representatives of the Class and their counsel as Class Counsel;

B. Award compensatory damages, including statutory damages where available, to Plaintiffs and the Class against Defendants for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Award restitution to Plaintiffs and the Class against Defendants;

D. Award punitive damages in an amount that will deter Defendants and others from like conduct;

E. Permanently restrain Defendants, and their officers, agents, servants, employees and attorneys, from tracking their users without consent or otherwise violating their policies with users;

F. Award Plaintiffs and the Class their reasonable costs and expenses incurred in this action, including counsel fees and expert fees;

G. Order that Defendants delete the data they collected about users through the unlawful means described above; and

H. Grant Plaintiffs such further relief as the Court deems appropriate.

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury of all issues so triable.

Dated: December 19, 2012

Respectfully submitted,

KEEFE BARTELS, LLC

/s/ Stephen G. Grygiel
Stephen G. Grygiel (Del Br No. 4944)
John E. Keefe, Jr.
Jennifer L. Harwood
170 Monmouth St.
Red Bank, NJ 07701
Tel: 732-224-9400
sgrygiel@keefbartels.com

Executive Committee Member

STRANGE & CARPENTER

/s/ Brian Russell Strange
Brian Russell Strange
Keith Butler
David Holop
12100 Wilshire Boulevard, Suite 1900
Los Angeles, CA 90025
Tel: 310-207-5055
lacounsel@earthlink.net

Executive Committee Member

BARTIMUS, FRICKLETON, ROBERTSON & GORNY, P.C.

/s/ James P. Frickleton
James P. Frickleton
Mary D. Winter
Stephen M. Gorny
Edward D. Robertston, Jr.
11150 Overbrook Road, Suite 200
Leawood, KS 66211
Tel: 913-266-2300
jimf@bflawfirm.com

Executive Committee Member

STEWARTS LAW US LLP

/s/ David A. Straite
David A. Straite (Del Bar No. 5428)
Ralph N. Sianni (Del Bar No. 4151)
Michele S. Carino (Del Bar. No. 5576)
Lydia E. York (Del Bar No. 5584)
1105 North Market Street
Wilmington, DE 19801
Tel: 302-298-1200
dstraite@stewartslaw.com

Plaintiffs' Steering Committee Member and Liaison Counsel

EICHEN, CRUTCHLOW, ZASLOW & MCELROY LLP

/s/ Barry Eichen
Barry R. Eichen
40 Ethel Road
Edison, NJ 08817
Tel: 732-777-0100
beichen@njadvocates.com

Plaintiffs' Steering Committee Member

SEEGER WEISS LLP

/s/ Jonathan Shub
Jonathan Shub
1515 Market Street, Suite 1380
Philadelphia, PA 19102
Tel: 215-564-2300
jshub@seegerweiss.com

Counsel for Plaintiff Lynne Krause and Plaintiffs' Steering Committee Member

MURPHY P.A.

/s/ William H. Murphy, Jr.
William H. Murphy, Jr.
One South Street, Suite 2300
Baltimore, MD 21202
Tel: 410-539-6500
billy.murphy@murphypa.com

Plaintiffs' Steering Committee Member

BARNES & ASSOCIATES

/s/ Jay Barnes
Jay Barnes
219 East Dunklin Street
Jefferson City, MO 65101
Tel: 573-634-8884
Jaybarnes5@gmail.com

Plaintiffs' Steering Committee Member

BRYANT LAW CENTER, PSC

/s/ Mark Bryant
Mark Bryant
601 Washington Street
P.O. Box 1876
Paducah, KY 42002-1876
Tel: 270-442-1422
mark.bryant@bryantpsc.com

Counsel for Plaintiff William G. Gourley and Plaintiffs' Steering Committee Member